模论讲义

MOLUN JIANGYI

贺昌亭　张同君

东北师范大学出版社

模 论 讲 义

贺昌亭　张同君

东北师范大学出版社

模 论 讲 义

MOLUN JIANGYI

贺昌亭　张同君

东北师范大学出版社出版　吉林省新华书店发行
（长春市斯大林大街110号）　长春市第四印刷厂印刷

开本：850×1168　1/32　印张：7　字数：178千
1987年12月第1版　　1987年12月第1次印刷
印数：1—4000册

ISBN 7—5602—0063—X/O.13
统一书号：13334·28（压膜）定价：1.50元

前　言

模论是抽象代数的基本而重要的组成部分，与代数学的许多分支有着密切的联系，是群论、环论极为重要的工具，同时也是同调代数、范畴理论以及代数拓扑的理论基础。作为一门课程，模论已被列入数学系代数选修课的首选课程之一。它与数学系两门必修的代数课程——高等代数、近世代数的联系相当密切。一方面，它以高等代数与近世代数的理论、方法作为全面的必要的基础，另一方面，又使得这些理论与方法得到充分的应用、补充和深化。特别是它把域上的有限维线性空间理论相当完美地发展成为主理想环上的有限生成模的理论。

本讲义的内容由两部分组成：模论基础和主理想环上有限生成模的基本理论及其在两个具体方面的应用——有限生成交换群的结构与域上有限维线性空间的一个线性变换的标准形问题。前者主要介绍作为一般的代数体系的模的基本概念、基本理论和方法；后者主要给出主理想环上有限生成模的结构定理：标准分解式的存在及其唯一性。在此基础上，对自同态的表示矩阵给出了具体的刻画，同时介绍了结构定理在两个具体问题上的应用。根据现行教学计划的要求，我们在讲义中安排的内容用50课时便可讲完。

作为一门选修课的讲义，本书在编写时着重考虑了两个方面的问题。首先，既要通过本讲义确切地传授模论的基本知识，更要在提高读者的代数学素质和掌握代数学方法上多花些工夫。其次，象其他代数课程一样，模论也有内容（概念、理论和方法）相当抽象、推理论证较多等特点。对此，我们尽量做到在文字叙述上详略适度，使之通俗易懂，简练明瞭。尤其是对每一个问题

的提出、分析和解决，既注意讲清楚“是什么”更注意讲透彻“为什么”，以便读者做到心中有数，目的明确，步骤清楚，从而知其然，也知其所以然。针对内容抽象、论证较多的特点，我们配置了数量充分、各有针对性的例题，又使许多重要而又繁难的论证用例题简单地再现出来。因此，可以说讲义中的例题是本讲义不可缺少的重要组成部分。

由于我们的水平和经验所限，本讲义在科学性方面会有许多不足和谬误之处，希望大家予以指正。

编　者

于东北师范大学数学系

1986年9月

目　录

第1章

模论基础

在这一章里介绍模论的基础知识，包括以下三个方面：

1. 模的概念；子模与商模

2. 模的映射；同态定理和同构定理

3. 模的分解；Jordan—Hölder 定理和 Krull—Schmidt定理。

本章主要目的在于把域上线性空间的“有限维”这一特殊性质推广到一般的模上去。

§1 模的定义和例子

在高等代数和抽象代数这两门基础课程里，大家都已熟知数域（或一般域）F 上线性空间这一重要而基本的概念，它是这样一种代数体系：

（Ⅰ）假设F是域，V是加法群。

（Ⅱ）规定了一个F与V到V里的"倍数乘法"，即$\forall k\in F,\alpha\in V$使得

$$(k,\ \alpha)\longmapsto k\alpha\in V$$

（Ⅲ）满足以下四个运算规律：

(i) $k(\alpha+\beta)=k\alpha+k\beta$,

(ii) $(k+l)\alpha=k\alpha+l\alpha$,

(iii) $(kl)\alpha=k(l\alpha)$,

(iv) $1_F\alpha=\alpha$

其中 $k,\ l\in F,\ \alpha,\ \beta\in V,\ 1_F$ 为域F的恒等元素。

不难看出，在（Ⅲ）中要求成立的四条算律，并不直接需要F是域这一前提，甚至于就连F的乘法可交换性也不是必须的。明显提出要求的只是域F中恒等元素 1_F 在倍数乘法之下的特殊作用。这样，把F是域减弱为F是一般的有恒等元素的环时，按照（Ⅰ）、（Ⅱ）和（Ⅲ）这三个方面的要求，便规定了比域F上线性空间更为广泛的代数体系——环上的模的概念。

定义 1 假设

（Ⅰ）R为有恒等元素1_R（$\neq 0$）的环，M是加法群。

（Ⅱ）规定了一个R与M到M里的倍数乘法：

$\forall k\in R,\ \alpha\in M$使 $(k,\ \alpha)\longmapsto k\alpha\in M$.

（Ⅲ）具有以下四条运算性质：

(i) $k(\alpha+\beta)=k\alpha+k\beta$,

(ii) $(k+l)\alpha=k\alpha+l\alpha$,

(iii) $(kl)\alpha=k(l\alpha)$

(iv) $1_R\alpha=\alpha$,

其中 k, $l\in R$, $\alpha,\beta\in M$, 1_R为环R的恒等元素，那么就称M做成环R上的一个左模．也说M是一个左R—模．

特别地，当R是域时，域上的模就是通常的线性空间．

用数学归纳法，根据定义1容易直接推出左—R模M如下的简单性质．

1，$k(\alpha_1+\alpha_2+\cdots+\alpha_n)=k\alpha_1+k\alpha_2+\cdots+k\alpha_n$,

2，$(k_1+k_2+\cdots+k_n)\alpha=k_1\alpha+k_2\alpha+\cdots+k_n\alpha$,

3，$(-k)\alpha=-(k\alpha)=k(-\alpha)$,

4，$0\alpha=0=k0$

下面列出模的一些例子．

例 1

1，偶数加法群 M 做成整数环 **Z** 上的一个左模；有理数加法群 $\{$**Q**$;\ +\}$ 也做成整数环 **Z** 上的左模．但是，整数加法群 $\{$**Z**$;\ +\}$ 不能做成偶数环R上的模，同时整数加法群也不做成有理数域**Q**上的左模（习题11）．

2，数域F上一元多项式的加法群 $M=\{F[x];\ +\}$ 做成整数环 **Z**上的模；做成数域 F 上的模；也做成多项式环 $F[x]$ 上的模．

3，考虑数域F上的n阶方阵环$R=\{M_n(F);\ +,\cdot\}$，令加法群$M=\{M_n(F);\ +\}$．于是这样一个加法群M可以分别是左 **Z**—模；左F—模；左R—模．

4，考虑六个元素的剩余类环 $\mathbf{Z}_6=\{\overline{0},\overline{1},\overline{2},\overline{3},\overline{4},\overline{5}\}$，令加法群$M=\{\mathbf{Z}_6;\ +\}$．于是加法群 M 可以分别是左 **Z**—模；左 $\mathbf{Z}_6$—模．如果取 $R=\{\overline{0},\overline{2},\overline{4}\}$，做为 $\mathbf{Z}_6$ 的子环，R本身是一个环，而且有恒等元素$1_R=\overline{4}$．于是按照 $\mathbf{Z}_6$中的乘

法，R与M到M里有一个倍数乘法。试问这时加法群$M=\{\mathbf{Z}_6;+\}$是否做成一个左R—模，为什么？

例 2 任一加法群M均可按自然方式成为整数环 $\mathbf{Z}$上的模，即 $\mathbf{Z}$与M到M里的倍数乘法规定如下：

$$na=\begin{cases} a+a+\cdots+a(n\text{个}a), & \text{当}n>0\text{时}, \\ 0, & \text{当}n=0\text{时}, \\ -|n|a, & \text{当}n<0\text{时}, \end{cases}$$

由加法群中的倍数算律，可知M是左 $\mathbf{Z}$—模。

例 3 设R为任一有恒等元素的环，M 为 R的一个左理想，于是，把环的乘法取做R与M到M里的倍数乘法，这样 M 做成一个左R—模。

特别地，取M为环R的加法群$\{R;+\}$时，那么R的加法群$M=\{R;+\}$可自然的看成是左R—模。

例 4 设R_0是有恒等元素的环，R 为 R_0 的一个子环，使$1_{R_0}\in R$。那么任一R_0 上的左模 M都可自然地看成子环 R 上的左模。特别地，R_0的加法群$\{R_0;+\}$可按自然方式看成一个左R—模。

例 5 设R是有恒等元素的环。对积集

$$R^{(n)}=\{(x_1,x_2,\cdots,x_n)|x_i\in R,\ i=1,2,\cdots,n\}$$

规定

$$\begin{aligned}&(x_1,x_2,\cdots,x_n)+(y_1,y_2,\cdots,y_n)\\ =&(x_1+y_1,x_2+y_2,\cdots,x_n+y_n),\\ &k(x_1,x_2,\cdots,x_n)\\ =&(kx_1,kx_2,\cdots,kx_n).\end{aligned}$$

那么$R^{(n)}$做成环R上的一个左R—模。

例 6 设R为有恒等元素的环。N为自然数集合。对从N到R的一切映射组成的集合

$$R^N=\{f\mid f:N\to R\}$$

规定

$$(f+g)(n)=f(n)+g(n),$$
$$(kf)(n)=kf(n)\ ,$$
其中f, $g\in R^N$, $k\in R$, $n\in N$, 那么R^N做成环R上的一个左模。

例 7 设V是域F上的线性空间，σ为V的一个取定的线性变换，$F[x]$是F上的一元多项式环。于是，规定$F[x]$与V到V里的倍数乘法如下：

$$\forall f(x)\in F[x],\ \alpha\in V\ 使得\ f(x)\alpha=f(\sigma)(\alpha)$$
那么V做成多项式环$F[x]$上的左模。

事实上 令 $f(x)=a_0+a_1x+\cdots+a_nx^n$，按倍数乘法的定义，则有

$$\begin{aligned}f(x)\alpha&=(a_0+a_1x+\cdots+a_nx^n)\alpha\\&=(a_0\sigma^0+a_1\sigma+\cdots+a_n\sigma^n)(\alpha)\\&=a_0\sigma^0(\alpha)+a_1\sigma(\alpha)+\cdots+a_n\sigma^n(\alpha)\end{aligned}$$
这样，所谓 $f(x)$ 与 α 相乘的结果就是用线性变换 σ 导出的线性变换 $f(\sigma)$ 去作用向量 α 所得的结果。于是，根据线性变换的运算性质容易指出V确实做成多项式环 $F[x]$ 上的一个左模。

象上面这样，从域F上的一个线性空间 V，通过一个线性变换 σ，得到的 $F[x]$ 一模 V在后面的讨论中还要用到，把它叫做由线性变换 σ 导出的模。

在本节最后对两个问题说明如下。

首先，模是线性空间概念的自然发展。因此模的理论中有许多结果是线性空间相应事实的推广。但模毕竟不同于线性空间，从而线性空间理论中的某些事实，对于模来说不再成立。

例如

$$k\alpha=0\Longleftrightarrow k=0或\alpha=0,$$
这一线性空间中尽人皆知的简单事实，在模中则未必成立。这可由$\mathbf{Z}$—模 $\mathbf{Z}_6$ 得到说明：

$$6\in\mathbf{Z},\ \ 6\neq 0,\ \ \overline{2}\in\mathbf{Z}_6,\ \ \overline{2}\neq\overline{0},\ 可是\ 6\ \overline{2}=\overline{0}。$$

其次，我们给出的模概念突出了一个左字，叫做左 R——模。

这是因为倍数乘法是环 R 的元素从左边去乘加法群M中的元素的缘故。从而完全类似地有右 R——模的概念。即

定义1′ 假设

（Ⅰ′）R是有恒等元素的环，M是加法群。

（Ⅱ′）规定了一个M与R到M的倍数乘法，即

$\forall\ \alpha\in M,\ k\in R$，使 $(\alpha,\ k)\longmapsto \alpha k\in M$。

（Ⅲ′）满足以下四个运算规律：

(i)′ $(\alpha+\beta)k=\alpha k+\beta k$,

(ii)′ $\alpha(k+l)=\alpha k+\alpha l$,

(iii)′ $\alpha(kl)=(\alpha k)l$,

(iv)′ $\alpha 1_R=\alpha$

其中 $\alpha,\ \beta\in M,\ k,\ l\in R$，$1_R$为环$R$的恒等元素，那么就称$M$做成环$R$上的一个右模，也说$M$是一个右$R$—模。

可以指出，对具体的模来说，左 R—模与右R—模确有区别。例如，取

$$R=\left\{\begin{pmatrix}a&0\\b&c\end{pmatrix}\middle|\ a,\ b,\ c\in \mathbf{Z}_2\right\},\quad M=\left\{\begin{pmatrix}0&x\\0&y\end{pmatrix}\middle|\ x,\ y\in \mathbf{Z}_2\right\}$$

把矩阵乘法取做倍数乘法，那么M是左 R——模，但是，M 不能做成右R——模。因为这时右倍数乘法在 M 上不是封闭的。如果，把左倍数乘法就规定为右倍数乘法，即令

$$\alpha \circ k\equiv k\alpha,\ \forall k\in R,\ \alpha\in M.$$

这样，运算"$\circ$"确实是M与R到M的一个右倍数乘法运算。但是，令

$$\alpha=\begin{pmatrix}0&1\\0&1\end{pmatrix},\quad k=\begin{pmatrix}0&0\\1&1\end{pmatrix},\quad l=\begin{pmatrix}1&0\\1&1\end{pmatrix}$$

则有

$$\alpha\circ(kl)=(kl)\,\alpha=\left[\begin{pmatrix}0&0\\1&1\end{pmatrix}\begin{pmatrix}1&0\\1&1\end{pmatrix}\right]\begin{pmatrix}0&1\\0&1\end{pmatrix}=\begin{pmatrix}0&0\\0&1\end{pmatrix},$$

$$(\alpha\circ k)\circ l=l(k\alpha)=\begin{pmatrix}1&0\\1&1\end{pmatrix}\left[\begin{pmatrix}0&0\\1&1\end{pmatrix}\begin{pmatrix}0&1\\0&1\end{pmatrix}\right]=\begin{pmatrix}0&0\\0&0\end{pmatrix},$$

故而

$$a\circ(kl)\neq(a\circ k)\circ l.$$

所以，取右倍数乘法为$a\circ k\equiv ka$时，M不做成右R—模。

显然，当R为交换环时，对任一左（右）R—模M，令

$$a\circ k\equiv ka\quad(k\circ a\equiv ak)$$

时，M也是一个右（左）R—模。因为有

$$a\circ(kl)=(kl)a=(lk)a=l(ka)=(a\circ k)\circ l.$$

$$\Big((kl)\circ a=a(kl)=a(lk)=(al)k=k\circ(l\circ a)\Big).$$

一般地，令R^C表示环R之反环。即在加法群$\{R;\ +\}$中，取

$$x\circ y\equiv yx,\quad\forall x,\ y\in R,$$

为乘法运算，则有$\{R;\ +,\ \circ\}$做成一个新的环R^C。它在恒等映射之下与原来的环R反同构。明显地，R是交换环$\Longleftrightarrow\{R;\ +,\ \cdot\}=\{R;\ +,\ \circ\}$，即$R=R^C$。

这样，如果M是左R—模，令

$$a\circ k\equiv ka,\quad\forall k\in R^C,\ a\in M.$$

则M做成右R^C—模。

事实上　由$(kl)a=k(la)$成立，可有

$$a\circ(k\circ l)=(k\circ l)a=(lk)a=l(ka)=(a\circ k)\circ l.$$

即

$$a\circ(k\circ l)=(a\circ k)\circ l,\quad\forall k,\ l\in R^C,\ a\in M.$$

而且反过来也成立，即如果M是右R—模，令

$$k\circ a\equiv ak,\quad\forall k\in R^C,\ a\in M,$$

则M做成左R^C—模。

由此看来，环上的左模理论与右模理论是对称的。因而以下仅就左R—模进行讨论。并且为了简便，对R上的左模M，略去左字而称为R—模。当在叙述中所指的环R是清楚的时候，把R—模M也可简称为模M。

本节主要讲了两个问题：模的定义和模的一些基本例子。学

习要领是根据定义验证例子，通过例子理解定义。

习　　题

1. 设M是左R—模，f是环S到R的同态映射，使S的恒等元素（$\neq 0$）的象是R的恒等元素。

证明：如果规定

$$\forall k\in S,\ a\in M,\ 使\ ka\equiv f(k)a,$$

那么M做成环S上的模。

2. 设M是R—模，$B=\{k\in R\mid ka=0,\ \forall a\in M\}$

证明

(i) B是R的理想。

(ii) 若C是R的理想，$C\subseteq B$，规定

$$(k+C)a\equiv ka,\ \forall\ k+C\in R/C,\ a\in M.$$

那么M做成R/C上的模（这里的B叫做模M在R中的零化子）。

3. 设R为实数域，令$V=R^{(n)}=\{(x_1,\ x_2,\ \cdots,x_n)\mid x_i\in R\}$为$R$上的$n$元行空间．取$V$的线性变换

$$\sigma:(x_1,\ x_2,\ \cdots,\ x_n)\longmapsto(x_n,\ x_1,\ \cdots,\ x_{n-1}),$$

于是按照

$$f(x)a\equiv f(\sigma)a,\ \forall a\in V,$$

V做成多项式环$R[x]$上的模，从而确定

(i) xa,

(ii) $(x^2+2)a$,

(iii) $(x^{n-1}+x^{n-2}+\cdots+x+1)a$,

(iv) 满足 $(x^2-1)a=0$ 的一切 a,

(v) V在$R[x]$中的零化子$B=\{f(x)\in R[x]\mid f(x)a=0,\ \forall a\in V\}$.

4. 设

$$R=\left\{\begin{pmatrix} a & 0 \\ b & c \end{pmatrix} \middle| a, b, c\in \mathbf{Z}_2\right\}.$$

加法群

$$M=\left\{\begin{pmatrix} 0 & x \\ 0 & y \end{pmatrix} \middle| x, y\in \mathbf{Z}_2\right\},$$

试规定一个M与R到M的右倍数乘法，使M做成右R—模.

5. 设M是n元加法群，$\mathbf{Z}_n$是n元剩余类环.

证明：

(i) $\overline{m}\,a=ma$, $\forall\,\overline{m}\in\mathbf{Z}_n$, $a\in M$

是$\mathbf{Z}_n$与M到M的一个倍数乘法.

(ii) 按上述倍数乘法，M做成$\mathbf{Z}_n$上的模.

6. 设S为非空集合，R是有恒等元素的环. 令F是S到R的一切映射f的集合，这里f使得S中只有有限个元素s在f之下的象不等于零：$f(s)\neq 0$. 证明，按如下规定的运算：

(i) $(f+g)(s)=f(s)+g(s)$, $\forall\, f, g\in F$, $s\in S$,

(ii) $(kf)(s)=kf(s)$, $\forall k\in R$, $f\in F$, $s\in S$,

F做成R上的模.

7. 设$\{M_i|i\in I\}$是一组R—模. 映射

$$f: I\longrightarrow \bigcup_{i\in I} M_i,\ 使f(i)\in M_i$$

令M为一切这样的映射组成的集合. 证明，按运算：

(i) $(f+g)(i)=f(i)+g(i)$, $\forall f, g\in M$, $i\in I$,

(ii) $(kf)(i)=kf(i)$ $\quad\forall k\in R$, $f\in M$, $i\in I$,

M做成R—模.

8. 设M为任一加法群. 证明：有且只有一种方法使M做成整数环$\mathbf{Z}$上的模.

9. 设M是有理数域$\mathbf{Q}$上的模. 证明这个模的倍数乘法是使M做成$\mathbf{Q}$—模的唯一的倍数运算.

10. 设M是有限加法群. M能否做成有理数域$\mathbf{Q}$上的模，为什么?

11. 能否规定一个倍数运算，使整数加法群$\mathbf{Z}$做成有理数域$\mathbf{Q}$上的模?

12. 设F为p个元素的有限域，p为素数. 整数加法群$\mathbf{Z}$能否做成F上的模?

13. 证明左R—模定义中之算律$1_R\alpha=\alpha$不能由定义中的其它条件推出.

14. . 试讨论左R—模定义中运算规律（Ⅲ）里四个条件的独立性.

15. 举例说明，对一个有恒等元素的环R和一个加法群M，可能有不同的两个倍数乘法都使M做成R—模.

16. 设M是加法群，其中每一个元素的阶均为素数p的幂. 环$R=\left\{\frac{a}{b}\in\mathbf{Q}\mid(b,\ p)=1\right\}$. 证明，$R$与$M$可用自然的方法定义倍数乘法使$M$做成$R$—模.

§2 加法群的自同态环

在前一节里，从大家熟悉的线性空间出发比较自然的引出了模的一般概念，为了对于一个加群M能够做成环R上的模的意义有更加一般的认识，在这一节里，我们讨论加法群的自同态及其一些基本性质。

设M为任一加法群。M到M的一个同态映射φ叫做M的一个自同态。即

$$\varphi: M \longrightarrow M,$$
$$\varphi: \alpha \longmapsto \alpha',$$
$$\beta \longmapsto \beta',$$

都有$\varphi(\alpha+\beta)=\alpha'+\beta'$，$\forall \alpha, \beta \in M$。

命题 1 设M为加法群，$EndM$表示M的一切自同态组成的集合。规定

$$(\varphi_1+\varphi_2)(\alpha)=\varphi_1(\alpha)+\varphi_2(\alpha),$$
$$(\varphi_1\varphi_2)(\alpha)=\varphi_1(\varphi_2(\alpha)), \quad \forall \varphi_1, \varphi_2 \in EndM.$$

那么$\{EndM;\ +,\cdot\}$做成环，M的恒等自同态是它的恒等元素。

证 由于问题比较简单、明确，因此证明的具体步骤和细节略而不写。只是强调一点，即，首先须要指明的是两个自同态φ_1，φ_2之和$\varphi_1+\varphi_2$还是加群M的自同态：$\forall \varphi_1, \varphi_2 \in EndM \Longrightarrow \varphi_1+\varphi_2 \in EndM$。至于$\varphi_1$与$\varphi_2$的积（合成）也是$M$的自同态，这似乎可以认为是已知的。▌

称$EndM$的任一子环为M的一个自同态环。

命题 2 设R为有恒等元素的环。那么R同构于一个加法群的自同态环。

证 取加法群$M=\{R;\ +\}$。对环R的每一个元素a，确定

的一个变换：

$$a_l: \alpha \longmapsto a\alpha,\quad \forall \alpha\in M.$$

于是，

$$a_l(\alpha+\beta)=a(\alpha+\beta)=a\alpha+a\beta=a_l(\alpha)+a_l(\beta).$$

这说明 a_l 是加群 M 的一个自同态，即 $a_l\in EndM$。令 $R_l=\{a_l \mid a\in R\}$，即R_l为由R中一切元素所确定的“左倍数”变换做成的集合。我们将指出：$R\simeq R_l$。

为此，首先说明R_l是M的一个自同态环，即R_l是$EndM$的子环。

$\forall a_l,\ b_l\in R_l,\implies (a_l+b_l)(\alpha)=a_l(\alpha)+b_l(\alpha)=a\alpha+b\alpha=(a+b)\alpha=(a+b)_l(\alpha)$。所以$a_l+b_l\in R_l$。完全类似地，可知 $a_l-b_l\in R_l$。

再有，$(a_lb_l)(\alpha)=a_l(b_l(\alpha))=a(b\alpha)=(ab)\alpha=(ab)_l(\alpha)$。所以，$a_lb_l\in R_l$。这就说明了，$R_l$是$EndM$的一个子环。

其次，在R与R_l之间建立一个映射，令

$$\eta:\ a\longmapsto a_l,\quad \forall a\in R.$$

于是，自然容易得到：

$$\eta:\ a+b\longmapsto (a+b)_l=a_l+b_l,$$
$$ab\longmapsto (ab)_l=a_lb_l$$

即η是从R到R_l的环同态。显然可见，η是R到R_l的满射，故而 $R\overset{\text{满}}{\sim}R_l$。

最后指出η的核$ker\eta=\{0\}$。

因为$a\in ker\eta\iff a_l$是零同态$\iff\forall\alpha\in M$，$a_l(\alpha)=a\alpha=0$。取$\alpha=1_R\in M$时，则得$a=0$。这样，$R\overset{\text{满}}{\simeq}R_l$。∎

命题 3 设M为任一加法群，R为M的一个自同态环，含有恒等自同态。那么，M便可按自然的方式做成环R上的模，即规定倍数乘法为

$$k\alpha\equiv k(\alpha),\quad \forall\, k\in R,\ \alpha\in M,$$

时，M便成为R上的模。

证明是非常明白的，故而略去。▌

定理 设R为有恒等元素的环，M是加法群，于是

（1）如果M做成R上的模，那么R同态于M的一个自同态环，而且R的恒等元素对应于M的恒等自同态。

（2）如果R同态于M的一个自同态环，使其恒等元素对应于M的恒等自同态，那么M便可自然的成为R上的一个模。

证 （1）对环R的每一个元素k，我们确定加法群M的一个自同态：

$$k_l: a \longmapsto ka, \quad \forall a \in M.$$

令

$$\varphi: k \longmapsto k_l, \quad \forall k \in R$$

则有

$$\varphi(k+h)=\varphi(k)+\varphi(h),\ \varphi(kh)=\varphi(k)\varphi(h),$$

即φ是从R到$EndM$里的一个环同态映射。从而R同态于M的一个自同态环。

（2）设环R同态于M的一个自同态环R'：

$$R \overset{\varphi}{\sim} R',\ \text{且}\ \varphi(1_R)=id_M.$$

于是，便可自然的规定一个R与M到M的倍数乘法：

$$ka \equiv \varphi(k)(a),\ \forall k \in R,\ a \in M.$$

而且

（i）$k(a+\beta)=\varphi(k)(a+\beta)=\varphi(k)(a)+\varphi(k)(\beta)=ka+k\beta$

（ii）$(k+h)a=\varphi(k+h)(a)=(\varphi(k)+\varphi(h))(a)=\varphi(k)(a)+\varphi(h)(a)=ka+ha$

（iii）$(kh)a=\varphi(kh)(a)=(\varphi(k)\varphi(h))(a)=\varphi(k)(\varphi(h)(a))=k(ha)$,

（iv）$1_R a=\varphi(1_R)(a)=id_M(a)=a$

这样，M做成了环R上的一个模。▌

例1 确定整数加法群$\mathbf{Z}$的自同态环$End\mathbf{Z}$。

首先找出 $\mathbf{Z}$ 的一切自同态。因为 $\mathbf{Z}=\langle 1\rangle$ 是循环群，所以 $\mathbf{Z}$ 的任一自同态 σ 由它对生成元素 1 的象 $\sigma(1)$ 所唯一决定。若令 $\sigma(1)=r$，记 $\sigma=\sigma_r$，
则有

$$\sigma_r(m)=\sigma_r(m\cdot 1)=m\cdot\sigma_r(1)=rm,\ \forall m\in\mathbf{Z}.$$ 而且，$\forall r\in\mathbf{Z}$，映射

$$\sigma: m\longmapsto rm$$

都是 $\mathbf{Z}$ 的一个自同态，使 $\sigma(1)=r$。所以 $\sigma=\sigma_r$。这样，σ_r $(r=0,\ \pm1,\ \pm2,\ \cdots)$ 恰是 $\mathbf{Z}$ 的全部自同态，即
$End\mathbf{Z}=\{\sigma_r|\sigma_r(1)=r,\ r=0,\ \pm1,\ \pm2,\ \cdots\}$.

其次定出环 $End\mathbf{Z}$ 的结构。令

$$\eta: \sigma_r\longmapsto r,$$

则 η 是 $End\mathbf{Z}$ 与 $\mathbf{Z}$ 之间的一个双射，并且

$$(\sigma_r+\sigma_s)(1)=\sigma_r(1)+\sigma_s(1)=r+s,$$
$$(\sigma_r\sigma_s)(1)=\sigma_r(\sigma_s(1))=\sigma_r(s)=rs$$

即

$$\eta: \sigma_r+\sigma_s\longmapsto r+s,$$
$$\sigma_r\sigma_s\longmapsto rs.$$

所以 $End\,\mathbf{Z}\simeq\mathbf{Z}$，换句话说，整数加法群 $\mathbf{Z}$ 的自同态环 $End\mathbf{Z}$ 与整数环是同构的。

例 2 确定剩余类加群 $\mathbf{Z}_n$ 的自同态环 $End\,\mathbf{Z}_n$。

和例 1 完全类似，$\mathbf{Z}_n=\langle\overline{1}\rangle$ 是循环群。因此，$\mathbf{Z}_n$ 的任一自同态 σ 由它对生成元素 $\overline{1}$ 的象 $\sigma(\overline{1})$ 所唯一决定。若令 $\sigma(\overline{1})=\overline{r}\,(0\leqslant r<n)$，记 $\sigma=\sigma_{\overline{r}}$。则有

$$\sigma_r(\overline{m})=\sigma_{\overline{r}}(m\cdot\overline{1})=m\sigma_{\overline{r}}(\overline{1})=m\overline{r}=\overline{r}\,\overline{m}.$$

而且，$\forall\overline{r}\in\mathbf{Z}_n$，映射

$$\sigma: \overline{m}\longmapsto\overline{r}\overline{m}$$

都是加群 $\mathbf{Z}_n$ 的一个自同态，使 $\sigma(\overline{1})=\overline{r}$，即 $\sigma=\sigma_{\overline{r}}$。这样，$\sigma_{\overline{r}}$，$\overline{r}=\overline{0}$，$\overline{1}$，…，$\overline{n-1}$，恰是 $\mathbf{Z}_n$ 的全部自同态，即 $End\mathbf{Z}_n = \{\sigma_{\overline{r}} | \sigma_{\overline{r}}(\overline{1})=\overline{r}, \overline{r}\in\mathbf{Z}_n\}$。

进而，映射：

$$\eta: \sigma_{\overline{r}} \longmapsto \overline{r}$$

是 $End\mathbf{Z}_n$ 与 $\mathbf{Z}_n$ 之间的一个双射，并且不难指出 η 是环同构映射，所以 $End\mathbf{Z}_n \overset{\circ}{\simeq} \mathbf{Z}_n$。换句话说，剩余类加群 $\mathbf{Z}_n$ 的自同态环 $End\mathbf{Z}_n$ 与剩余类环 $\mathbf{Z}_n$ 是同构的。

例 3 设加法群 $M=\mathbf{Z}^{(2)}=\{(x, y)|x, y\in\mathbf{Z}\}$。确定 M 的自同态环 $EndM$。

令 $e_1=(1, 0)$，$e_2=(0, 1)$，则有 $(x, y)=xe_1+ye_2$。这说明 M 是两个元素 e_1，e_2 生成的群：$M=\langle e_1, e_2\rangle$。于是 M 的任一自同态 σ 由它对生成元素 e_1，e_2 的象 $\sigma(e_1)$，$\sigma(e_2)$ 所唯一决定。若令

$$\sigma(e_1)=f_1, \ \sigma(e_2)=f_2$$

$$\Longrightarrow \quad \sigma((x, y))=\sigma(xe_1+ye_2)=x\sigma(e_1)+y\sigma(e_2)=xf_1+yf_2$$

记 $\sigma=\sigma_{(f_1, f_2)}$，则有 $\sigma_{(f_1, f_2)}(e_1)=f_1$，$\sigma_{(f_1, f_2)}(e_2)=f_2$。一般地

$$\sigma_{(f_1, f_2)}((x, y))=xf_1+yf_2, \ \forall (x, y)\in M.$$

这表明，M 的每一个自同态 σ 都对应有 M 中的两个元素 f_1，f_2，使其为生成元素 e_1，e_2 在 σ 之下的象：$\sigma(e_1)=f_1$，$\sigma(e_2)=f_2$。

反之，事先任意给定 M 中的两个元素 u_1，u_2，必有 M 的唯一的一个自同态 τ，使在上述意义下，τ 所对应的两个元素恰是 u_1，u_2。事实上，令

$$\tau: (x, y)\longmapsto xu_1+yu_2, \ 即 \tau((x, y))=xu_1+yu_2,$$

则容易指出，τ 是加群 M 的一个自同态，并且

$$\tau(e_1)=u_1, \ \tau(e_2)=u_2,$$

即$\tau=\tau_{(u_1, u_2)}$

以上讨论表明加法群$M=\mathbf{Z}^{(2)}$的全部自同态恰好和M的积集合$M^{(2)}=\mathbf{Z}^{(2)}\times\mathbf{Z}^{(2)}$的元素成一一对应。即，令

$$EndM=\left\{\sigma_{(f_1, f_2)}\,\middle|\,\sigma_{(f_1, f_2)}(e_i)=f_i,\ f_i\in M,\ i=1,\ 2\right\}$$

及

$$\eta:\sigma_{(f_1, f_2)}\longmapsto(f_1,\ f_2),\ f_1,\ f_2\in M$$

则η是$EndM$与$M^{(2)}$之间的一个双射。

进而为了决定$EndM$的结构——它是个什么样的环，我们须要把$M^{(2)}$的表现形式改变一下，即对$M^{(2)}$中任一元素$(f_1,\ f_2)$，由于$f_1,\ f_2\in M=\mathbf{Z}^{(2)}$，故有$f_1=(a,\ b)$，$f_2=(c,\ d)$，$a, b, c,\ d\in\mathbf{Z}$。这样，我们就可以把$f_i$的分量当列元素，从而把元素$(f_1,\ f_2)$改写成为一个二阶方阵：

$$\begin{pmatrix} a & c \\ b & d \end{pmatrix}$$

按此办法，集合$M^{(2)}$就改变写法而变成了二阶方阵的集合

$$M_2(\mathbf{Z})=\left\{\begin{pmatrix} a & c \\ b & d \end{pmatrix}\,\middle|\,a,\ b,\ c,\ d\in\mathbf{Z}\right\}.$$

这样一来，前边指出的$EndM$与$M^{(2)}$之间的一一对应关系就转变成为$EndM$与$M_2(\mathbf{Z})$之间的一一对应关系，即

$$\eta:\sigma_{(f_1, f_2)}\longmapsto\begin{pmatrix} a & c \\ b & d \end{pmatrix},\ f_1=(a,\ b),\ f_2=(c,\ d).$$

有了这样的准备，很容易指出：映射η正是一个环同构映射。

事实上 若

$$\eta:\sigma\longmapsto\begin{pmatrix} a & c \\ b & d \end{pmatrix};\ \tau\longmapsto\begin{pmatrix} a' & c' \\ b' & d' \end{pmatrix}$$

$\Longrightarrow\sigma(e_1)=(a,\ b)$，$\sigma(e_2)=(c,\ d)$，$\tau(e_1)=(a',\ b')$，
$\tau(e_2)=(c',\ d')$。

$$\Longrightarrow (\sigma+\tau)(e_1)=\sigma(e_1)+\tau(e_1)=(a,\ b)+(a',\ b')$$

$$=(a+a',\ b+b').$$

$$(\sigma+\tau)(e_2)=\sigma(e_2)+\tau(e_2)=(c,\ d)+(c',\ d')$$

$$=(c+c',\ d+d')$$

以及 $(\sigma\tau)(e_1)=\sigma(\tau(e_1))=\sigma((a',\ b'))=a'(a,b)+b'(c,d)$

$$=(a'a,\ a'b)+(b'c,\ b'd)$$

$$=(a'a+b'c,\ a'b+b'd)$$

同理可得， $(\sigma\tau)(e_2)=(c'a+d'c,\ c'b+d'd)$

亦即

$$\sigma\tau \longmapsto \begin{pmatrix} a'a+b'c & c'a+d'c \\ a'b+b'd & c'b+d'd \end{pmatrix}=\begin{pmatrix} a & c \\ b & d \end{pmatrix}\begin{pmatrix} a' & c' \\ b' & d' \end{pmatrix}$$

这就是说：

$$\sigma+\tau \longmapsto \begin{pmatrix} a & c \\ b & d \end{pmatrix}+\begin{pmatrix} a' & c' \\ b' & d' \end{pmatrix},$$

$$\sigma\tau \longmapsto \begin{pmatrix} a & c \\ b & d \end{pmatrix}\begin{pmatrix} a' & c' \\ b' & d' \end{pmatrix},$$

$\Longrightarrow EndM \overset{\eta}{\simeq} M_2(\mathbf{Z})$， 其中$\eta$： $\sigma_{(f_1,f_2)} \longmapsto \begin{pmatrix} a & c \\ b & d \end{pmatrix}$，

$f_1=(a,\ b)$， $f_2=(c,\ d)$。

例 4 设V是域F上的线性空间，σ为V的一个线性变换，在上一节，根据模的原始定义我们指出，利用σ从F一空间V导出一个多项式环$F[x]$上的模V。此中使$x\alpha\equiv\sigma(\alpha)$。

现在，根据本节的定理，很简便的就可说明V确可成为环$F[x]$上的模，而使$x\alpha\equiv\sigma(\alpha)$。

事实上，线性变换σ自然是加法群V的一个自同态，而$F[\sigma]=\{a_0\sigma^0+a_1\sigma+\cdots+a_n\sigma^n \mid a_i\in F\}$是$V$的一个自同态环，并在映射

$$\eta: f(x)\longmapsto f(\sigma)\ ,$$

之下，使$F[x]$与$F[\sigma]$同态：$F[x]\overset{\eta}{\sim}F[\sigma]$。这样由本节定理，

加法群V便可自然的做成环$F[x]$上的模，此处之倍数乘法是

$$f(x)\alpha=f(\sigma)(\alpha).$$

这正是由线性变换σ导出的$F[x]$—模V。

习　　题

1．设$\{G;\ \cdot\}$为任一群，令F为G的一切变换$f: G\to G$的集合．把变换的合成做为F的乘法．另外规定加法如下：

$$(f+g)(x)=f(x)g(x),\ \forall x\in G,$$

试讨论代数体系$\{F;\ +,\ \cdot\}$的性质．

2．设M为加法群．$EndM$为M的自同态环．那么，M的一切自同构做成$EndM$的一个乘法子群$AutM$．对$\mathbf{Z}$、$\mathbf{Z}_n$确定自同构群$Aut\mathbf{Z}$与$Aut\mathbf{Z}_n$．

3．确定自同构群$Aut\mathbf{Z}^{(2)}$．

4．设$M=\mathbf{Z}^{(n)}=\{(x_1,\ x_2,\ \cdots,\ x_n)\mid x_i\in\mathbf{Z}\}$．确定自同态环$EndM$和自同构群$AutM$．

5．确定自同态环$End\mathbf{Q}$和自同构群$Aut\mathbf{Q}$．此处$\mathbf{Q}$是有理数加法群．

6．已经看到，对$\mathbf{Z}$、$\mathbf{Z}_n$都有$End\mathbf{Z}\simeq\mathbf{Z}$，$End\mathbf{Z}_n\simeq\mathbf{Z}_n$，一般地，对任一环$R$是否也有加法群$\{R;\ +\}$的自同态环$EndR\simeq R$，当$R$是域时如何？

7．设R为有恒等元素的环．$M=\{R;\ +\}$．在$EndM$里证明：$C(R_l)=R_r$，$C(R_r)=R_l$．此处$R_r=\{a_r\mid a_r: \alpha\mapsto\alpha a,\ a\in R,\ \alpha\in M\}$．

§3 子　　模

在抽象代数理论中，代数体系的子体系有普遍的重要意义。因此，模的子模自然也是模论中不可缺少的重要概念。

本节介绍子模的定义、例子和基本性质。

定义 1 设M是R—模，N是M的非空子集，如果用模M的加法和倍数乘法，N本身也做成R上的模，则称N是M的一个子模。

显然，对任一R—模M，$N_1=\{0\}$，$N_2=M$均为M的子模，叫做M的平凡子模。如果子模$N\neq M$，就说N是M的真子模。

命题 设M是R—模，N是M的非空子集。那么下列条件是等价的：

(1) N是M的子模。

(2) $\forall\alpha,\ \beta\in N,\ k\in R$　都有$\alpha+\beta\in N,\ k\alpha\in N$。

(3) $\forall\alpha,\ \beta\in N,\ k,\ l\in R$　都有$k\alpha+l\beta\in N$。

证 (1) $\Longrightarrow$(2)．这是自明的。

(2) $\Longrightarrow$(3)．$\forall\alpha,\ \beta\in N,\ k,\ l\in R$，都有$k\alpha\in N$，$l\beta\in N$。进而又有$k\alpha+l\beta\in N$。

(3) $\Longrightarrow$(1)．$\forall\alpha,\ \beta\in N,\ k,\ l\in R$，由$k\alpha+l\beta\in N$，令$k=1,\ l=-1$，则有$\alpha-\beta\in N$。这说明子集$N$是加法群$M$的子群。又令$l=0$，则有$k\alpha\in N$。这表明$M$的倍数乘法在子集$N$上是可施行的。这样，子集$N$用$M$的加法、倍数乘法做成$R$上的模，即$N$是$M$的子模。∎

如果对模M的一个非空子集S，具有性质：$\forall\alpha,\ \beta\in S\Longrightarrow\alpha+\beta\in S$，则称$S$在加法之下是封闭的，或者说$M$的加法在$S$上的

限制也是S的加法。若$\forall \alpha \in S$，$k \in R \Longrightarrow k\alpha \in S$，则称$S$在倍数乘法之下是封闭的，或者说倍数乘法在$S$上的限制也是$S$的倍数乘法。于是，上述命题说明，模$M$的非空子集$N$是$M$的子模$\Longleftrightarrow N$在加法、倍数乘法之下是封闭的。

下面列出子模的一些例子。

例 1 把任一交换群M看成 $\mathbf{Z}$—模。于是，M的非空子集N是M的子模$\Longleftrightarrow N$是交换群M的子群。

例 2 设R为有恒等元素的环。令$M = \{R; +\}$看成环R上的左模。于是，M的非空子集N是M的子模$\Longleftrightarrow N$是环R的左理想。

例 3 令$M = \{(x_1, x_2, \cdots, x_n, \cdots) \mid x_i \in \mathbf{Z}, i = 1, 2, \cdots\}$，按通常的运算方法，$M$做成整数环$\mathbf{Z}$上的模。取

$N_1 = \{(x_1, x_2, \cdots, x_n, \cdots) \mid$只有有限个$x_i \neq 0\}$；

$N_2 = \{(x_1, x_2, \cdots, x_m, 0, 0, \cdots) \mid m$为固定的自然数$\}$

那么，N_1与N_2都是M的子模。

例 4 对任一R—模M，$\alpha \in M$。子集

$$N = \{r\alpha \mid r \in R\}$$

是M的子模。

例 5 设V是域F上的线性空间。σ是V的一个取定的线性变换。那么

（1）V的一个非空子集N是F—模V的一个子模$\Longleftrightarrow N$是线性空间V的一个子空间。

（2）考虑由σ导出的$F[x]$—模V（§1、例7）。那么，V的一个非空子集N是$F[x]$—模V的一个子模$\Longleftrightarrow N$是线性变换σ的不变子空间。（注意：$\sigma(\alpha) = x\alpha$，$\forall \alpha \in V$）。

下面我们讨论如何从模M的一个子集得到一个子模。

定义 2 设M为R—模，S是M的一个子集。M的一个子模N如果满足条件：

（i）$S\subseteq N$，

（ii）对M的任一子模K，若$S\subseteq K$则$N\subseteq K$，

则称子模 N 是由子集S生成的子模。记作$N=\langle S\rangle$。

容易看出，子集S生成的子模$\langle S\rangle$是模M里包含子集 S 的一切子模当中最小的一个。而且

$$\langle S\rangle=S\Longleftrightarrow S\text{本身是}M\text{的子模}.$$

这表明，M的任一子模都可认为是生成的子模。

定理 1 设 $\{N_i \mid i\in I\}$ 是 R—模M的一组子模。那么这组子模的交

$$N=\bigcap_{i\in I}N_i$$

也是M的子模。

证 $\forall k,\ l\in R,\ \alpha,\ \beta\in N\Longrightarrow\alpha,\ \beta\in N_i\ (i\in I)$。$N_i$均为子模$\Longrightarrow\forall i\in I,\ k\alpha+l\beta\in N_i\Longrightarrow k\alpha+l\beta\in N$。这样，$N$是$M$的一个子模。▌

推论 设S为R—模M的任一子集，M中包含着 S 的一切子模的集合$\{N_i|N_i$是M的子模，且$S\subseteq N_i\}$，那么 $\cap N_i=\langle S\rangle$。即对任一子集$S$，生成子模都是存在的，而且只有一个。

证 令$N=\cap N_i$，根据定理1，N是M的一个子模，且$S\subseteq N$。若K为M的一个子模，$S\subseteq K$，那么K就是某一个子模N_i，因而，$N\subseteq K$。这样，由生成子模的定义，$\langle S\rangle=N=\cap N_i$。▌

为了具体的表示出$\langle S\rangle$的构成形式，我们给出以下的

定义 3 设 S 为 R—模 M 的任一非空子集。$\alpha_1,\ \alpha_2,\ \cdots,\ \alpha_r\in S,\ k_1,\ k_2,\ \cdots,\ k_r\in R$，则称$M$中的元素

$$\beta=k_1\alpha_1+k_2\alpha_2+\cdots+k_r\alpha_r$$

为 S中元素 $\alpha_1,\ \alpha_2,\ \cdots,\ \alpha_r$的线性组合，或者说，$\beta$ 可用 S 线性表出。

令$LC(S)=\{k_1\alpha_1+k_2\alpha_2+\cdots+k_r\alpha_r|\alpha_i\in S,\ k_i\in R,\ r$为任一自然数$\}$。

定理 2 设M为R—模，$S\subseteq M$。那么

$$\langle S\rangle=\begin{cases}\{0\}, & 当 S=\phi,\\ LC(S), & 当 S\neq\phi.\end{cases}$$

证 首先，当$S=\phi$时，M的每一个子模都包含着S，从而这一切子模的交就是子模$\{0\}$。

即$\langle S\rangle=\langle\phi\rangle=\{0\}$。

其次，当$S\neq\phi$时，则有

（i）$LC(S)$是M的一个子模，且$S\subseteq LC(S)$、

（ii）对M的任一子模K，若$S\subseteq K\Longrightarrow LC(S)\subseteq K$。这样，$LC(S)$恰好就是$S$生成的子模，即$\langle S\rangle=LC(S)$。▌

定理 3 设$\{N_i\mid i\in I\}$是R—模M的一组子模，$S=\bigcup\limits_{i\in I}N_i$。那么

$$\langle S\rangle=\{a_{t_1}+a_{t_2}+\cdots+a_{t_r}\mid a_{t_j}\in N_{t_j},\ j=1,2,\cdots,r\}.$$

证 只须指出两点：

（i）$N=\{a_{t_1}+a_{t_2}+\cdots+a_{t_r}\mid a_{t_j}\in N_{t_j},j=1,2,\cdots,r\}$

是M的一个子模。

（ii）若K为任一包含着并集$S=\bigcup\limits_{i\in I}N_i$的子模，则有$N\subseteq K$。

这样，N就是S生成的子模。即$\langle S\rangle=N$。▌

明显可见，$\langle\bigcup\limits_{i\in I}N_i\rangle$恰由$N_i(i\in I)$中元素的一切有限和所组成。记作$\langle\bigcup\limits_{i\in I}N_i\rangle=\sum\limits_{i\in I}N_i$，叫做这组子模的和。

特别地，当$S=N_1\cup N_2\cup\cdots\cup N_r$时，则有

$$\langle S\rangle=\{a_1+a_2+\cdots+a_r\mid a_i\in N_i,\ i=1,2,\cdots,r\}.$$

这时记作$\langle S\rangle=N_1+N_2+\cdots+N_r$。

例 6 对R—模M的任二子模N_1，N_2，我们都有$N_1\cap N_2$与

N_1+N_2 还是 M 的子模。但并集 $N_1\cup N_2$ 则未必也是子模。例如，令 $M=\mathbf{Z}^{(2)}=\{(x,\ y)|x,\ y\in\mathbf{Z}\}$ 是一个 $\mathbf{Z}$—模。于是 $N_1=\{(x,\ 0)|x\in\mathbf{Z}\}$，$N_2=\{(0,\ y)|y\in\mathbf{Z}\}$ 是 M 的两个子模。但是，明显可见，并集 $N_1\cup N_2$ 不是M的子模，一般地，容易指出：R—模M的两个子模N_1，N_2的并集 $N_1\cup N_2$是M的子模 $\Longleftrightarrow N_1\subseteq N_2$或$N_2\subseteq N_1$。

事实上，充分性是明显的。下面指出必要性。

若已知 $N_1\cup N_2$是一个子模，然而 $N_1\not\subseteq N_2$，$N_2\not\subseteq N_1$。$\Longrightarrow$ 存在 $a_1\in N_1$，但 $a_1\bar{\in}N_2$；存在 $a_2\in N_2$，但 $a_2\bar{\in}N_1$。于是 a_1，$a_2\in N_1\cup N_2$，而$N_1\cup N_2$是子模$\Longrightarrow a_1+a_2\in N_1\cup N_2$。$\Longrightarrow a_1+a_2\in N_1$或者$a_1+a_2\in N_2$。

由 $a_1+a_2\in N_1\Longrightarrow a_2=(a_1+a_2)-a_1\in N_1$，这与 $a_2\bar{\in}N_1$ 矛盾。而由 $a_1+a_2\in N_2\Longrightarrow a_1=(a_1+a_2)-a_2\in N_2$，这与 $a_1\bar{\in}N_2$矛盾。这样，当 $N_1\cup N_2$是 M 的子模时，必有 $N_1\subseteq N_2$ 或者$N_2\subseteq N_1$。

下面考虑用子集生成子模的一种特殊的而重要的情况。

设 $S=\{a_1,\ a_2,\ \cdots,\ a_n\}$ 是 R—模M的一个有限子集，则称$\langle S\rangle$为有限生成子模。a_1，$a_2,\cdots,a_n$叫做$\langle S\rangle$的一组生成元素，简记作$\langle S\rangle=\langle a_1,a_2,\cdots,a_n\rangle$。当$M=\langle a_1,\ a_2,\ \cdots,\ a_n\rangle$时，就说$M$是有限生成模。特别地，$n=1$ 时，则称$\langle S\rangle=\langle a_1\rangle$为$M$的循环子模。而当$M=\langle a_1\rangle$时，就说$M$是循环模。

显然，循环模是循环群的自然推广。可是二者确实有些差别。

例 7　如果N是R—模M的循环子模：$N=\langle a\rangle$，那么

$$N=\{ra|r\in R\},$$

简记作$N=Ra$。具体地，令 $R=M_2(\mathbf{Q})$ 为有理数域$\mathbf{Q}$上的二阶方阵环。那么，$M=\{R,\ +\}$ 做为R上的模是循环的，并且对任一 $a\in M$，当行列式$|a|\neq 0$ 时，都有 $M=\langle a\rangle=Ra$。但是，$M=\{R,\ +\}$ 也可以看成有理数域$\mathbf{Q}$上的模、整数环$\mathbf{Z}$上的模。

这时，二者都不是循环模。

例 8 设M为R—模。如果M做为加法群是循环群，那么R—模M必是循环模。反之，如R—模M是循环模，那么做为加法群的M则未必是循环群。前者是明显的。对于后者，把有理数域$\mathbf{Q}$看成$\mathbf{Q}$上的模时是循环模，但做为加法群来看时，$\{\mathbf{Q};+\}$则不是循环群。

例 9 整系数的一元多项式环$\mathbf{Z}[x]$，既可以看成$\mathbf{Z}$—模，也可以看成$\mathbf{Z}[x]$—模。不难指出，前者不是循环模，而后者则是循环模：

$\forall f(x)\in\mathbf{Z}[x]$，$\mathbf{Z}[x]\neq\mathbf{Z}f(x)$；而$\mathbf{Z}[x]=\mathbf{Z}[x]\cdot 1$。进而考虑，做为$\mathbf{Z}[x]$—模来看时，$\mathbf{Z}[x]$的子模。取子集$S=\{2, x\}$，则得子模$N=\langle 2, x\rangle$。我们已知，$N=\langle 2, x\rangle$不是环$\mathbf{Z}[x]$的主理想，从而它不是$\mathbf{Z}[x]$—模$\mathbf{Z}[x]$的循环子模。这样，可见循环模的子模未必还是循环模。

例10 设M为R—模，S为M的任一非空子集。令

$$ann(S)=\{k\in R\mid\forall a\in S,\ ka=0\}.$$

那么，不难指出$ann(S)$是环R的一个左理想，叫做S在R中的零化子。当S是子模时，它的零化子$ann(S)$是R的理想。特别地，对于交换环R上的循环子模$S=\langle\alpha\rangle$，如果$\langle\alpha\rangle=\langle\beta\rangle\Longrightarrow ann(\{\alpha\})=ann(\{\beta\})$。进而对于$\mathbf{Z}$—模$M$来说，$ann(\langle\alpha\rangle)=(n)$，其中的$n$恰是生成元素$\alpha$在加法群$M$里的阶（周期）。因而循环子模$\langle\alpha\rangle$的零化子$ann(\langle\alpha\rangle)$也叫做$\langle\alpha\rangle$的阶理想。并简记作$ann(\langle\alpha\rangle)=ann\alpha$，或者记作$0(\alpha)$（习题11）。

下面证明关于子模的交与和的一个重要性质来结束这一节的讨论。

定理 4 设M是R—模，A，B，C都是M的子模，且$C\subseteq A$。那么

$$A\cap(B+C)=(A\cap B)+C.$$

证 一方面，因为$C\subseteq A$，$\Longrightarrow A+C=A$。又因为

$$(A\cap B)+C\subseteq A+C, \ (A\cap B)+C\subseteq B+C$$

$$\Longrightarrow (A\cap B)+C\subseteq (A+C)\cap(B+C)=A\cap(B+C).$$

另一方面，$\forall\alpha\in A\cap(B+C)$，$\Longrightarrow\alpha\in A$ 且 $\alpha=\beta+\gamma$，其中 $\in B$，$\gamma\in C$。由于$C\subseteq A$，则$\gamma\in A$。从而 $\beta=\alpha-\gamma\in A$，$\Longrightarrow\beta\in A\cap B$。这样，$\alpha=\beta+\gamma\in(A\cap B)+C$，即$A\cap(B+C)\subseteq(A\cap B)+C$。所以，$A\cap(B+C)=(A\cap B)+C$。▮

习　　题

1. 设M为R—模，R是交换环。令$\forall r\in R$，

$$rM=\{r\alpha\mid\forall\alpha\in M\},$$

$$M_r=\{\alpha\in M\mid r\alpha=0\},$$

证明：

（i）rM，M_r都是M的子模。

（ii）取$R=\mathbf{Z}$，$M=\mathbf{Z}_n$，当$n=st$，$(s, t)=1$时，$sM=M_t$。

2. 设$\{M_i\mid i\in I\}$是R—模M的一组子模。如对指标集I的每一有限子集 J，存在$k\in I$，使得

$$\bigcup_{i\in J}M_j\subseteq M_k,$$

那么 $\bigcup_{i\in I}M_i=\sum_{i\in I}M_i$。

3. 上题的逆是否成立？

4. 设M是R—模，A，B，C是M的子模，使得

$$A\subseteq B, \ A+C=B+C, \ A\cap C=B\cap C.$$

证明：$A=B$。

5. 设M是R—模，证明：

（i）如果S是环R的左理想，那么

$$SM=\left\{\sum_{i=1}^{m}s_ia_i\,\middle|\,s_i\in S,\ a_i\in M\right\}$$

是M的一个子模。

（ii）如S是环R的右理想，那么

$$S_0=\{a\in M\mid\forall s\in S,\ sa=0\}$$

是M的一个子模。

6. 把域F上线性空间V看成F—模，证明：V的一个子模 S是循环的$\Longleftrightarrow S$做为子空间，$\dim S\leqslant 1$。

7. 证明：有理数加法群 $\mathbf{Q}$，做为 $\mathbf{Z}$—模来看不是有限生成的。

8. 令 $\mathbf{Q}_p=\left\{\frac{n}{m}\in\mathbf{Q}\,\middle|\,p\text{为取定的素数},\ m=p^s,\ s\geqslant 0\right\}$.

证明：$\mathbf{Q}_p$是$\mathbf{Z}$—模$\mathbf{Q}$的子模，并且求出$\mathbf{Q}$的一切子模N，使 $\mathbf{Z}\subseteq N\subseteq\mathbf{Q}_p$。

9. 设R为主理想环。证明：R上循环模$M=\langle a\rangle$ 的每一个子模N都是循环子模。

10. 举例说明，如果R—模 M是有限生成的，但是做为加法群的M则不是有限生成的。

11. 设M为R—模。α，$\beta\in M$。

（i）如果$\langle\alpha\rangle=\langle\beta\rangle$，是否必有$ann\alpha=ann\beta$?

（ii）如果 R是可换环，则有：$\langle\alpha\rangle=\langle\beta\rangle\Longrightarrow ann\alpha=ann\beta$。举例说明，反之则不成立。

（iii）如果R是可换环，那么 $ann\alpha$ 是 R 的一个理想，并且$\langle\alpha\rangle=\langle\beta\rangle\Longleftrightarrow\beta=k\alpha$，其中$\bar{k}$在剩余环$R/ann\alpha$里是可逆元素。

12. 设R为有恒等元素、没有零因子、可换的环。M是R上的模。证明：

（i）令$N=\{a\in M\mid ann\,a\neq\{0\}\}$，那么$N$是 M的一个子模（称N为M的扭子模，记作$N=T(M)$）。

（ii）如果去掉R没有零因子的条件，（i）的结论是否还成立？

13. 设M是主理想环R上的模。证明：

（i）$\alpha, \beta \in M$，若$ann\alpha \neq \{0\}$，$ann\beta \neq \{0\}$，那么，$ann(\alpha+\beta) \neq \{0\}$。

（ii）令$ann\alpha=(a)\neq\{0\}$，$ann\beta=(b)\neq\{0\}$，$ann(\alpha+\beta)=(c)\neq\{0\}$。那么$c \backslash \frac{ab}{(a,b)}$，$\frac{ab}{(a,b)^2} \backslash c$，其中$(a,b)$表示$a$与$b$的最大公因子。

14. 设M为R—模。那么，M是有限生成的$\Longleftrightarrow M$中不存在无限真递增的子模序列：

$$M_1 \subset M_2 \subset M_3 \subset \cdots.$$

即，对子模的任一递增序列

$$M_1 \subseteq M_2 \subseteq M_3 \subseteq \cdots,$$

必有k，使得$M_k=M_{k+1}=\cdots$。

15. 设$R=\{(a_1, a_2, \cdots, a_n, \cdots) \mid a_i \in \mathbf{Z}\}$。按通常的运算方式规定$R$的加法和乘法：

$$(x_1,\cdots,x_n,\cdots)+(y_1,\cdots,y_n,\cdots)=(x_1+y_1,\cdots,x_n+y_n,\cdots),$$

$$(x_1,\cdots,x_n,\cdots)\cdot(y_1,\cdots,y_n,\cdots)=(x_1y_1,\cdots,x_ny_n,\cdots).$$

证明：

（i）R做成有恒等元素的环。

（ii）取$M=\{R;+\}$，那么M看成R上的模时是循环模。

（iii）求出M的一个子模N，使N不是有限生成的R—模。

§4 同态映射

在抽象代数理论中，同态映射的重要作用是相当明显的、突出的.对此,我们也是比较熟悉的. 它的意义在于把有着某些共性的代数体系联系起来加以比较. 由此对于两个同态的代数体系，便可从当中的一个去认识、掌握另外一个. 这样做不仅是抽象代数的一种方法，也是抽象代数的一种特殊的风格和基本思想.

本节介绍模的同态映射概念及其基本性质. 这些结果在以后的讨论中都经常的起着重要作用.

定义 1 设M，M'都是R—模，φ是从M到M'的一个映射，即

$$\varphi: \alpha \longmapsto \alpha', \quad \forall \alpha \in M.$$

如果

(i) $\varphi(\alpha+\beta)=\varphi(\alpha)+\varphi(\beta)$,

(ii) $\varphi(k\alpha)=k\varphi(\alpha)$, $\forall \alpha, \beta \in M$, $k \in R$.

则称φ是模M到M'的一个同态映射，或者说φ是M到M'的一个R—同态。当$M=M'$时，φ叫做M的一个R—自同态.

设φ是M到M'的一个R—同态.

如果φ是单射，则称φ为R—单同态.

如果φ是满射，则称φ为R—满同态. 这时也说模 M 与 M' 同态，记作$M \overset{\varphi}{\sim} M'$.

如果φ是双射，则称φ为R—同构，这时也说模M与M'同构，记作 $M \overset{\varphi}{\simeq} M'$. 当然，按代数的观点，两个同构的模没有实质性的区别，可以认为是相同的模.

用数学归纳法可以证明，对M中任意一组元素α_1，α_2，…，

α_n及$k_1, k_2, \cdots, k_n \in R$，则有

$$\varphi(k_1\alpha_1+k_2\alpha_2+\cdots+k_n\alpha_n)$$
$$=k_1\varphi(\alpha_1)+k_2\varphi(\alpha_2)+\cdots+k_n\varphi(\alpha_n)$$

例 1 设M，M'都是加法群，于是M，M'都可看成**Z**—模。那么，M到M'的一个**Z**—同态φ就是M到M'的群同态，反之亦然。

例 2 设V，V'都是域F上的线性空间。那么，V到V'的F—同态φ就是线性空间V到线性空间V'的线性映射。特别地，当$V=V'$时，V的F—自同态恰是V的线性变换。

例 3 设R为有恒等元素的环。于是R可以看成R—模。这时，R的模同态与R的环同态一般来说是不一样的。

令

$$R=\left\{\begin{pmatrix} a & b \\ c & d \end{pmatrix} \middle| \ a,\ b,\ c,\ d \in \mathbf{Q}\right\}$$

$$t: \begin{pmatrix} a & b \\ c & d \end{pmatrix} \longmapsto t\begin{pmatrix} a & b \\ c & d \end{pmatrix},\ t\in\mathbf{Q},\ t\neq 0,\ 1.$$

容易验证，映射t是R—模$\{R;\ +\}$的一个R—自同态。但它不是环R的环自同态。

再有，把复数域**C**看成**C**上的模，映射

$$\varphi: \alpha \longmapsto \overline{\alpha},\ \forall \alpha\in\mathbf{C},$$

是**C**的环自同态。但它不是模**C**的自同态。这是因为，

$$\varphi: k\alpha \longmapsto \overline{k\alpha}=\overline{k}\ \overline{\alpha},$$

然而，$\overline{k}\ \overline{\alpha}=k\overline{\alpha}$不是对任意的$k\in\mathbf{C}$都成立的。

例 4 设M_1，M_2都是R—模。且M_1是有限生成的：$M_1=\langle\alpha_1, \alpha_2, \cdots, \alpha_n\rangle$，如果$\varphi$是$M_1$到$M_2$的一个$R$—同态，则有$M_2$中的一组确定的元素$\beta_1, \beta_2, \cdots, \beta_n$，使$\varphi(\alpha_1)=\beta_1$，$\varphi(\alpha_2)=\beta_2$，$\cdots$，$\varphi(\alpha_n)=\beta_n$。于是$M'=\langle\beta_1, \beta_2, \cdots, \beta_n\rangle$是$M_2$的一个子模。这时，如果在$M_1$与$M'$之间来看，$\varphi$就是$M_1$到$M'$的一个$R$—满同态，即有$M_1 \overset{\varphi}{\sim} M'$。

反之，若预先取定M_2的一组元素 $r_1, r_2, \cdots, r_n$. 是否必有唯一的一个M_1到M_2的R—同态ψ，使得 $\psi(\alpha_1)=r_1$，$\psi(\alpha_2)=r_2$，$\cdots$，$\psi(\alpha_n)=r_n$？

例 5 令$M=R^{(n)}=\{(x_1, x_2, \cdots, x_n)|x_i\in R\}$是环$R$上的模。那么

$$e_i: (x_1, \cdots, x_i, \cdots, x_n)\longmapsto x_i,$$

是$R^{(n)}$到R的R—满同态。

$$\tau_i: x\longmapsto(0, \cdots, 0, x, 0, \cdots, 0),$$

其中 x 在第 i 个位置上，那么τ_i是R到$R^{(n)}$的R—单同态。

例 6 设M为R—模，N是M的子模。那么映射

$$\tau: \alpha\longmapsto\alpha, \ \forall\alpha\in N,$$

是N到M的一个R—单同态。称这样的R—同态为包含同态。

例 7 设V是域F上的线性空间，σ 是V的一个线性变换。考虑由 σ 导出的$F[x]$—模V。我们已经知道，线性空间 V的模自同态恰是V的线性变换。现在讨论 $F[x]$ —模 V 的模自同态有何特性。

令 τ 是$F[x]$—模V的任一模自同态。根据定义，则有

$$\tau(\alpha+\beta)=\tau(\alpha)+\tau(\beta), \ \forall\alpha, \ \beta\in V,$$

$$\tau(f(x)\alpha)=f(x)\tau(\alpha), \ \forall f(x)\in F[x], \ \alpha\in V.$$

特别地，则有

$$\tau(k\alpha)=k\tau(\alpha), \ \forall k\in F,$$

$$\tau(x\alpha)=x\tau(\alpha)$$

这表明：τ 是线性空间V的线性变换，而且

$$\tau(\sigma(\alpha))=\sigma(\tau(\alpha)),$$

亦即 $\tau\sigma=\sigma\tau$。这也就是说，$F[x]$—模V的任意一个 $F[x]$—自同态 τ 都是线性空间V的线性变换，并且 τ 与 σ 可交换。

反过来看，如果 τ 是线性空间V的线性变换，能与σ相交换：$\tau\sigma=\sigma\tau$。于是

$$\Longrightarrow \tau(\alpha+\beta)=\tau(\alpha)+\tau(\beta);$$

$\Longrightarrow \quad \tau(x\alpha)=\tau(\sigma(\alpha))=\sigma(\tau(\alpha))=x\tau(\alpha)$;

$\Longrightarrow \quad \tau(f(x)\alpha)=\tau(f(\sigma)(\alpha))=f(\sigma)(\tau\alpha)=f(x)\tau(\alpha)$.

这表明，τ 正是$F[x]$—模V的一个$F[x]$—自同态. 总之，$F[x]$—模V的全部 $F[x]$—自同态恰是线性空间V的一切与 σ 可交换的线性变换.

设M，M'都是R—模，φ是M到M'的 R—同态. 令X 是 M 的任一子集，Y是M'的任一子集. 于是

$$\varphi(X)\equiv\{\varphi(\alpha)\,|\,\alpha\in X\}$$

是M'的一个子集，叫做X在φ之下的象.

$$\varphi^{-1}(Y)\equiv\{\alpha\in M\,|\,\varphi(\alpha)\in Y\}$$

是M的一个子集，叫做Y在φ之下的完全原象.

定理 1 设M，M'都是 R—模，$\varphi: M\longrightarrow M'$是 R—同态. 那么

(1) 若N为M的子模，则$\varphi(N)$是M'的子模，

(2) 若N'是M'的子模，则$\varphi^{-1}(N')$ 是M的子模.

证 (1) $\forall\alpha'$，$\beta'\in\varphi(N)$，有α，$\beta\in N$，使

$$\varphi(\alpha)=\alpha',\ \varphi(\beta)=\beta'.$$

$\Longrightarrow\varphi(\alpha+\beta)=\varphi(\alpha)+\varphi(\beta)=\alpha'+\beta'$. 因为 $\alpha+\beta\in N$，所以 $\alpha'+\beta'\in\varphi(N)$.

$\Longrightarrow\varphi(k\alpha)=k\varphi(\alpha)=k\alpha'$，$\forall k\in R$，因为$k\alpha\in N$，所以$k\alpha'\in\varphi(N)$. $\Longrightarrow\varphi(N)$ 是M'的子模.

(2)同理，$\forall\alpha$，$\beta\in\varphi^{-1}(N')$，则有$\varphi(\alpha)\in N'$，$\varphi(\beta)\in N'$.
$\Longrightarrow\varphi(\alpha+\beta)=\varphi(\alpha)+\varphi(\beta)$，$\varphi(k\alpha)=k\varphi(\alpha)$. 因为$N'$是$M'$的子模，所以 $\varphi(\alpha)+\varphi(\beta)\in N'$，$k\varphi(\alpha)\in N'$. 从而可知 $\alpha+\beta\in\varphi^{-1}(N')$，$k\alpha\in\varphi^{-1}(N')$. 即$\varphi^{-1}(N')$ 是M的子模. ▌

推论 令$L(M)=\{N\subseteq M\,|\,N\text{是}M\text{的子模}\}$是$M$的一切子模的集合；$L(M')=\{N'\subseteq M'\,|\,N'\text{是}M'\text{的子模}\}$ 是M'的一切子模的集合. 那么 M到 M'的任意一个模同态 φ，考虑 φ 在子模上的作用 则有

(1) $\varphi: L(M) \longrightarrow L(M')$，且使包含关系不变：

若N_1，$N_2 \in L(M)$，$N_1 \subseteq N_2 \Longrightarrow \varphi(N_1) \subseteq \varphi(N_2)$。

(2) $\varphi^{-1}: L(M') \longrightarrow L(M)$，且使包含关系不变：

若N'_1，$N'_2 \in L(M')$，$N'_1 \subseteq N'_2 \Longrightarrow \varphi^{-1}(N'_1) \subseteq \varphi^{-1}(N'_2)$。■

定义 2 设$\varphi: M \longrightarrow M'$ 是R—同态。则称$\varphi(M)$为φ的象，记作$Im\varphi$。称$\varphi^{-1}(0)$为φ的核，记作$ker\varphi$。

例8 若$\varphi: M \longrightarrow M'$是$R$—同态。则有

(1) φ是R—满同态$\Longleftrightarrow Im\varphi = M'$。

(2) φ是R—单同态$\Longleftrightarrow ker\varphi = \{0\}$。

例 9 如果对一组R—模：

$$M_0, M_1, \cdots, M_{i-1}, M_i, M_{i+1}, \cdots,$$

相应地存在一组R—同态：

$$\varphi_i: M_i \longrightarrow M_{i+1}, \quad i = 0, 1, 2, \cdots.$$

则称如下的记法为一个R—模与R—同态的序列：

$$\cdots \longrightarrow M_{i-1} \xrightarrow{\varphi_{i-1}} M_i \xrightarrow{\varphi_i} M_{i+1} \longrightarrow \cdots$$

如果对每三个相邻的模及R—同态都有

$$Im\varphi_{i-1} = ker\varphi_i, \quad i = 1, 2, \cdots,$$

则称该序列是**正合列**。显然，正合列的意思是说，对列中每一个模M_i来看，“输入同态”的象与“输出同态”的核正好重合。

特别地，把如下的正合列叫**短正合列**：

$$0 \longrightarrow M' \xrightarrow{\sigma} M \xrightarrow{\tau} M'' \longrightarrow 0,$$

其中“0”表示零模$\{0\}$；而$0 \longrightarrow M'$ 表示 自然包含同态，$M'' \longrightarrow 0$表示零同态。

于是，若$\varphi: M \longrightarrow N$是$R$—同态，则有

φ是R—单同态$\Longleftrightarrow 0 \longrightarrow M \xrightarrow{\varphi} N$是正合列，

φ是R—满同态$\Longleftrightarrow M \xrightarrow{\varphi} N \longrightarrow 0$是正合列。

φ是R—同构$\Longleftrightarrow 0 \longrightarrow M \longrightarrow N \longrightarrow 0$是正合列，

例10 设$\varphi: M \longrightarrow M'$是$R$—同态。$N$，$N'$分别是$M$，$M'$的子模。那么

(1) $\varphi^{-1}[\varphi(N)] = N + ker\varphi$,

(2) $\varphi[\varphi^{-1}(N')] = N' \cap Im\varphi$.

首先说明（1）成立。因为$ker\varphi = \varphi^{-1}(0)$，所以$ker\varphi \subseteq \varphi^{-1}[\varphi(N)]$。再有，$\forall \alpha \in N$，则有$\varphi(\alpha) \in \varphi(N)$，从而$\alpha \in \varphi^{-1}[\varphi(N)]$，这样$N \subseteq \varphi^{-1}[\varphi(N)]$。故得

$$N + ker\varphi \subseteq \varphi^{-1}[\varphi(N)]$$

另一方面，如果$\alpha \in \varphi^{-1}[\varphi(N)]$，则$\varphi(\alpha) \in \varphi(N)$。这表明有$\beta \in N$，使$\varphi(\alpha) = \varphi(\beta)$，$\Longrightarrow \alpha - \beta \in ker\varphi$，即，$\alpha \in N + ker\varphi$。故得$\varphi^{-1}[\varphi(N)] \subseteq N + ker\varphi$。这就证明了（1）成立。

其次说明（2）成立。显然可见$\varphi[\varphi^{-1}(N')] \subseteq N' \cap Im\varphi$。

另一方面，如果$\alpha' \in N' \cap Im\varphi$，于是有$\alpha \in M$，使$\varphi(\alpha) = \alpha' \in N'$。$\Longrightarrow \alpha \in \varphi^{-1}(N') \Longrightarrow \alpha' = \varphi(\alpha) \in \varphi[\varphi^{-1}(N')]$。即

$$N' \cap Im\varphi \subseteq \varphi[\varphi^{-1}(N')]$$

这就证明了（2）成立。

在本节最后，我们讨论R—同态的合成问题。

首先，如果$\sigma: M_1 \longrightarrow M_2$，$\tau: M_2 \longrightarrow M_3$都是$R$—同态。令

$$\tau\sigma: \alpha \longmapsto \tau[\sigma(\alpha)], \ \forall \alpha \in M_1,$$

那么容易验证$\tau\sigma$是从M_1到M_3的一个R—同态。称$\tau\sigma$为τ与σ的积。

事实上 $\forall \alpha, \beta \in M_1$，$k \in R$，则有

$$\begin{aligned}\tau\sigma(\alpha+\beta) &= \tau[\sigma(\alpha+\beta)] = \tau(\sigma(\alpha)+\sigma(\beta)) \\ &= \tau[\sigma(\alpha)] + \tau[\sigma(\beta)] = \tau\sigma(\alpha) + \tau\sigma(\beta), \\ \tau\sigma(k\alpha) &= \tau[\sigma(k\alpha)] = \tau[k\sigma(\alpha)] = k\tau[\sigma(\beta)] \\ &= k\tau\sigma(\alpha)\end{aligned}$$

即$\tau\sigma: M_1 \longrightarrow M_3$是一个$R$—同态。

若$\rho: M_3 \longrightarrow M_4$也是一个$R$—同态。则有

$$\rho(\tau\sigma) = (\rho\tau)\sigma,$$

这个等式说明R—同态的合成是可结合的，它的验证过程，我们略去不写。

这样，如果一般地用$Hom_R(M, N)$表示R—模M到R—模N的一切R—同态做成的集合，那么，特别地，R—模M的一切R—自同态的集合$Hom_R(M, M)$关于合成做为乘法时，组成一个有恒等元素的半群。其中恒等自同态

$$id_M: \alpha \longmapsto \alpha, \quad \forall \alpha \in M,$$

使得

$$id_M \sigma = \sigma = \sigma\, id_M, \quad \forall \sigma \in Hom_R(M, M).$$

即id_M是半群$Hom_R(M, M)$的恒等元素。

其次，在集合$Hom_R(M, N)$上规定加法如下：

$$(\sigma+\tau): \alpha \longmapsto \sigma(\alpha)+\tau(\alpha), \quad \forall \alpha \in M,$$

即

$$(\sigma+\tau)(\alpha)=\sigma(\alpha)+\tau(\alpha), \quad \forall \alpha \in M,$$

于是可以证明，关于这样定义的加法运算，集合$Hom_R(M, N)$做成一个加法群$\{Hom_R(M, N);+\}$。

对此，首先应该指出这个加法在$Hom_R(M, N)$上是可施行的（具有封闭性）。即$\forall \sigma, \tau \in Hom_R(M, N)$，则$\sigma+\tau \in Hom_R(M, N)$，换个说法就是，$M$到$N$的两个$R$—同态之和也是$M$到$N$的$R$—同态。

事实上，$\forall \alpha, \beta \in M, k \in R$，则有

$$\begin{aligned}(\sigma+\tau)(\alpha+\beta) &= \sigma(\alpha+\beta)+\tau(\alpha+\beta)\\ &= \sigma(\alpha)+\sigma(\beta)+\tau(\alpha)+\tau(\beta)\\ &= \sigma(\alpha)+\tau(\alpha)+\sigma(\beta)+\tau(\beta)\\ &= (\sigma+\tau)(\alpha)+(\sigma+\tau)(\beta).\end{aligned}$$

$$\begin{aligned}(\sigma+\tau)(k\alpha) &= \sigma(k\alpha)+\tau(k\alpha)\\ &= k\sigma(\alpha)+k\tau(\alpha)\\ &= k(\sigma(\alpha)+\tau(\alpha))\\ &= k(\sigma+\tau)(\alpha).\end{aligned}$$

这就说明 $\sigma+\tau$确实也是 M 到 N 的一个 R—同态。此外，关于 $\{Hom_R(M, N); +\}$ 满足加群的全部条件的验证，这里就略而不写了。

至此，对于任意一个R—模M，都相应的有一个代数体系 $\{Hom_R(M,M); +,\cdot\}$。它的全部元素是模M的一切R—自同态，两个运算分别是前面提到的加法和乘法。而且，单看加法是一个交换群；单看乘法是一个有恒等元素的半群。于是进而可想，如果乘法对加法适合分配律，$\{Hom_R(M, M); +, \cdot\}$ 就做成一个有恒等元素的环了。下面就来指出这一点。

设 $\sigma, \tau, \rho\in Hom_R(M, M)$，$\forall a\in M$，则有

$$\begin{aligned}\sigma(\tau+\rho)(a)&=\sigma[(\tau+\rho)(a)]=\sigma[\tau(a)+\rho(a)]\\&=\sigma[\tau(a)]+\sigma[\rho(a)]=\sigma\tau(a)+\sigma\rho(a)\\&=(\sigma\tau+\sigma\rho)(a),\end{aligned}$$

即 $\sigma(\tau+\rho)=\sigma\tau+\sigma\rho$，同样可得 $(\tau+\rho)\sigma=\tau\sigma+\rho\sigma$。

总括以上所述，我们证明了如下的结果，即

定理2 设M为R—模，那么 $\{Hom_R(M, M); +, \cdot\}$ 做成一个有恒等元素的环。▮

称 $\{Hom_R(M, M); +, \cdot\}$ 为R—模 M的自同态环，可以简记作End_RM。须要注意的，$EndM$ 是加法群M的自同态环，而这里的End_RM则是R—模M的自同态环。

习　　题

1．证明：

(1) 如果 $\sigma: M_1\to M_2$，$\tau: M_2\to M_3$都是R—满同态，那么$\tau\sigma$是M_1到M_3的R—满同态。

(2) 如果 $\sigma: M_1\to M_2$，$\tau: M_2\to M_3$都是R—单同态，那么

$\tau\sigma$是M_1到M_3的R—单同态。

(3) 如果 $\sigma: M_1 \to M_2$, $\tau: M_2 \to M_3$是R—同态，且$\tau\sigma$是R—满同态，那么σ是R—满同态，

(4) 如果 $\sigma: M_1 \to M_2$, $\tau: M_2 \to M_3$是R—同态，且$\tau\sigma$是R—单同态，那么τ是R—单同态。

2. 设R为有恒等元素的交换环。$\varphi: R^{(2)} \to R$为任一映射。证明：φ是一个R—同态$\Longleftrightarrow$存在$a, b \in R$，使得$\varphi((x, y)) = ax + by$。$\forall (x, y) \in R^{(2)}$。

3. 设M为R—模，$rM = \{r\alpha | \alpha \in M\}$是$M$的子模。令

$$\sigma_r: \alpha \mapsto r\alpha, \ \forall \alpha \in M,$$

那么

(1) 当r为环R的中心元素时，σ_r是模M与其子模rM的一个R—同态。

(2) 举例说明，r不是中心元素时，σ_r则未必是R—同态。

(3) 举一个例子，使σ_r是R—同构。这时，做为模M的同构象，子模rM是否与M相等？

4. 设$\varphi: M \to N$是R—同态。若A是M的子模，B是N的子模，则有

$$\varphi[A \cap \varphi^{-1}(B)] = \varphi(A) \cap B.$$

5. 设$M = \langle \alpha \rangle$，$N = \langle \beta \rangle$是$R$上的两个循环模。

证明：如果$ann\alpha \subseteq ann\beta$，那么$M \sim N$。

6. 设M，N为R—模，$M \sim N$，证明：

(1) M是循环模$\Longrightarrow$$N$是循环模，反过来对吗？

(2) M是有限生成的$\Longrightarrow$$N$是有限生成的，反过来对吗？

7. 把$\mathbf{Z}$，$\mathbf{Z}_n$，$\mathbf{Z}^{(2)}$都看成$\mathbf{Z}$—模。

(1) 求出加法群$Hom(\mathbf{Z}, \mathbf{Z}_n)$和$Hom(\mathbf{Z}_n, \mathbf{Z})$。

(2) 证明：$Hom(\mathbf{Z}^{(2)}, \mathbf{Z}) \simeq \{\mathbf{Z}^{(2)}; +\}$。

8. 证明：对任一R—模M，$Hom(R, M) \simeq \{M, +\}$。

9. 设M为R—模，$EndM$为加法群M的自同态环，$R_l = \{a_l \in$

$EndM|a_l: x\mapsto ax, \forall x\in M\}$。证明：模$M$的自同态环$End_RM$是$R_l$在$EndM$的中心化子：$End_RM=C(R_l)$。

10．对一般环R上的模M，加法群M的左倍数变换$a_l(a\in R)$是模M的R—同态吗？

11．设R为有恒等元素、没有零因子的交换环．证明：

（1）如果$\sigma: M\to N$是R—同态，那么$\sigma(T(M))\subseteq T(N)$，从而$\sigma$在$T(M)$上的限制$\sigma_T$是$T(M)$到$T(N)$的$R$—同态．其中$T(M)$表示$M$的扭子模。

（2）如果$0\longrightarrow M\xrightarrow{\sigma} N\xrightarrow{\tau} P$是正合列，那么

$$0\longrightarrow T(M)\xrightarrow{\sigma_T} T(N)\xrightarrow{\tau_T} T(P)$$

也是正合列。

（3）如果$\sigma: M\to N$是R—满同态，则$\sigma_T: T(M)\to T(N)$未必是R—满同态。

12．证明：

（1）如果$0\longrightarrow A\longrightarrow B\xrightarrow{\sigma} C\longrightarrow 0$，$0\longrightarrow C\xrightarrow{\tau} D\longrightarrow E\longrightarrow 0$都是短正合列，那么$0\longrightarrow A\longrightarrow B\xrightarrow{\tau\sigma} D\longrightarrow E\longrightarrow 0$是正合列。

（2）每个正合列都可以象（1）那样，由一些适当的短正合列粘接而成。

13．设A，B，C都是非空集合，映射$\sigma: A\to B$，$\tau: A\to C$。证明：存在映射$\rho: B\to C$，使$\rho\sigma=\tau\Longleftrightarrow\sigma(x)=\sigma(y)\Longrightarrow\tau(x)=\tau(y)$，$\forall x, y\in A$。举例说明，对一般的$R$—模$A$，$B$，$C$来说，这个结论未必成立。

14．设A，B，C都是非空集合，映射$\sigma: B\to A$；$\tau: C\to A$。证明：存在映射$\rho: C\to B$，使$\sigma\rho=\tau\Longleftrightarrow Im\sigma=Im\tau$。举例说明，对一般的$R$—模$A$，$B$，$C$来说，这个结论未必成立。

15. 设A, B, C都是R—模. $\sigma: A\to B$, $\tau: A\to C$是R—同态，其中σ是满同态. 证明：存在唯一的R—同态：$\rho: B\to C$，使$\rho\sigma=\tau \Longleftrightarrow ker\sigma\subseteq ker\tau$. 并且$ker\sigma=ker\tau\Longleftrightarrow\rho$是单同态.

16. 设A, B, C都是R—模，$\sigma: B\to A$, $\tau: C\to A$是R—同态. 其中σ是单同态. 证明：存在唯一的R—同态$\rho: C\to B$，使$\sigma\rho=\tau\Longleftrightarrow Im\tau\subseteq Im\sigma$，并且$Im\tau=Im\sigma\Longleftrightarrow\rho$是满同态.

17. 设A, B, C, D都是R—模，$0\to A\xrightarrow{\sigma}B\xrightarrow{\tau}C$是正合列，$R$—同态$\rho: D\to B$，使得$\tau\rho=0$，证明：存在唯一的$R$—同态$\eta: D\to A$，使$\sigma\eta=\rho$. 特别地，对$R$—同态$\sigma: M\to N$，包含同态$i: ker\sigma\to M$来说，如果任意的$R$—模$P$，$R$—同态$\tau: P\to M$，满足$\sigma\tau=0$. 则存在唯一的$R$—同态$\rho: P\to ker\sigma$，使得$i\rho=\tau$.

§5 商模 同构定理

本节讨论两个问题：商模的概念及其基本性质——同态基本定理和几个主要的同构定理。

设M为任一R—模．K是M的任一子模．于是，M做为交换群来看，K自然是M的正规子群．从而K给M划分成一个商群

$$M/K=\{\overline{\alpha}=\alpha+K\mid\alpha\in M\}.$$

此时，在M/K中的加法如下进行：

$$\overline{\alpha}+\overline{\beta}=\overline{\alpha+\beta},\ \forall\ \overline{\alpha},\ \overline{\beta}\in M/K.$$

在此基础上，我们可以想到，按如下方法对R与M/K到M/K规定一个倍数乘法，使M/K做成一个R—模．即$\forall k\in R$, $\overline{\alpha}\in M/K$，令

$$k\overline{\alpha}=\overline{k\alpha}.$$

首先必须指出，这样规定的运算方法是合理的．换句话说就是与$\overline{\alpha}$中代表元素的选取无关．事实上

若$\overline{\alpha}=\overline{\beta}\Longrightarrow\alpha-\beta\in K$, $k(\alpha-\beta)=k\alpha-k\beta\in K$.

$\Longrightarrow\overline{k\alpha}=\overline{k\beta}$，即$k\overline{\alpha}=k\overline{\beta}$．

这样，容易证明下述的结论．即

命题 设M是R—模，K是M的一个子模．那么，按如下的运算：

$$\overline{\alpha}+\overline{\beta}=\overline{\alpha+\beta},$$

$$k\overline{\alpha}=\overline{k\alpha},\ \forall k\in R,\ \overline{\alpha},\ \overline{\beta}\in M/K,$$

商集合M/K做成一个R—模．

证 $\{M/K;\ +\}$做成交换群是早已知道的．倍数乘法的合

理性已如前述。剩下的就是模定义中（Ⅱ）所要求的四条运算性质。这可逐条验证如下：

$$(\text{i})\ k(\overline{\alpha}+\overline{\beta})=k(\overline{\alpha+\beta})=\overline{k(\alpha+\beta)}=\overline{k\alpha+k\beta}=\overline{k\alpha}+\overline{k\beta}$$

$$=k\overline{\alpha}+k\overline{\beta}$$

$$(\text{ii})\ (k+l)\overline{\alpha}=\overline{(k+l)\alpha}=\overline{k\alpha+l\alpha}=\overline{k\alpha}+\overline{l\alpha}=k\overline{\alpha}+l\overline{\alpha}.$$

$$(\text{iii})\ (kl)\overline{\alpha}=\overline{(kl)\alpha}=\overline{k(l\alpha)}=k\overline{l\alpha}=k(l\overline{\alpha}).$$

$$(\text{iV})\ 1_R\overline{\alpha}=\overline{1_R\alpha}=\overline{\alpha}.$$

这样就证明了，加法群 $\{M/K;\ +\}$ 是R上的模。▌

称M/K为模M关于子模K的**商模**。

象群和环的同态基本定理一样，关于商模的重要意义，也有所谓的“模同态基本定理”。即

定理1 设M是一个R—模，K是M的一个子模。那么映射

$$\eta: \alpha \longmapsto \overline{\alpha},\quad \forall \alpha \in M,$$

是M到商模M/K的一个R—同态，而且是满同态，并且核$ker\eta$ 恰为子模K。即

$$\eta(\alpha)=\overline{\alpha}\ \text{使}\ M\overset{\eta}{\sim}M/K,\ \text{且}\ ker\eta=K.$$

反之，若：$\varphi: M\to M'$是R—满同态，$ker\varphi=K$，那么，映射

$$\overline{\varphi}: \overline{\alpha} \longmapsto \varphi(\alpha),\quad \forall \overline{\alpha} \in M/K$$

是商模M/K与M'的一个R—同构。即

$$\overline{\varphi}(\overline{\alpha})=\varphi(\alpha)\ \text{使}\ M/K\overset{\overline{\varphi}}{\simeq}M'.$$

证 先证第一个结论。我们注意到，商模M/K其实就是做为加法群的M关于正规子群K的商群 $\{M/K;\ +\}$，又规定了一个自然的倍数乘法：k 与陪集相乘就是 k 乘陪集中的每一个元素，得到的一个模。并且这里的映射 η 就是M与商群M/K的自然同态。这样，只要指出群同态 η 还满足 R—同态的第二条性质，这里的结论就完全被证明了。事实上有

$$\eta(ka)=\overline{ka}=k\overline{a}=k\eta(a),\quad \forall k\in R;\ a\in M.$$

（关于η的核，做为群同态来看或是做为R—同态来看是一回事情，所以$ker\eta=K$）。

再证第二个结论。由于同样的想法，这里的映射$\overline{\varphi}$是M/K与M'之间的双射，而且保持加法运算，即做为加法群来看，$\{M/K;\ +\}\overset{\overline{\varphi}}{\simeq}M'$。为了说明$\overline{\varphi}$还是一个$R$—同构，只须指出$\overline{\varphi}$也保持倍数乘法就行了。即

$$\overline{\varphi}(k\overline{a})=\overline{\varphi}(\overline{ka})=\varphi(ka)=k\varphi(a)=k\overline{\varphi}(\overline{a}),$$

$\forall k\in R,\ \overline{a}\in M/K$。这样，第二个结论也被证明了。

例1 考虑实数域$\mathbf{R}$上的三维空间$\mathbf{R}^{(3)}=\{(x,\ y,\ z)|x,\ y,\ z\in\mathbf{R}\}$。于是

$$\varphi:(x,\ y,\ z)\mapsto x$$

是$\mathbf{R}^{(3)}$到$\mathbf{R}$的一个$\mathbf{R}$—同态，而且是满同态。即

$$\mathbf{R}^{(3)}\overset{\varphi}{\sim}\mathbf{R}.$$

容易看出，$ker\varphi=\{(0,\ y,\ z)|y,\ z\in\mathbf{R}\}$，从而

$$\mathbf{R}^{(3)}/ker\varphi\overset{\overline{\varphi}}{\simeq}R,\quad \overline{\varphi}:\overline{(x,\ y,\ z)}\longmapsto\varphi((x,\ y,z))=x.$$

这里，对$\mathbf{R}^{(3)}/ker\varphi$的任二元素$\overline{(x,y,z)}$，$\overline{(x',\ y',\ z')}$有

$$\overline{(x,y,z)}=\overline{(x',\ y',\ z')}\Longleftrightarrow(x,\ y,\ z)-(x',\ y',\ z')\in$$

$ker\varphi\Longleftrightarrow x=x'$。从而，$\overline{(x,y,z)}=\overline{(x,0,0)}$。

例2 把有理数加法群$\mathbf{Q}$看成$\mathbf{Z}$—模。$\mathbf{Z}\subseteq\mathbf{Q}$是$\mathbf{Q}$的一个子模。那么商模

$$\mathbf{Q}/\mathbf{Z}=\{\overline{x}=x+\mathbf{Z}|x\in\mathbf{Q}\}.$$

令$x=[x]+\{x\}$，其中$[x]$与$\{x\}$分别表示有理数x的整数部分与小数部分。例如

$3.4=3+0.4$，即$[3.4]=3$，$\{3.4\}=0.4$；

$-2.8=-3+0.2$，即$[-2.8]=-3$，$\{-2.8\}=0.2$；

$5=5+0$，即$[5]=5$，$\{5\}=0$。

于是

$$\overline{3.4}=\overline{[3.4]+\{3.4\}}=\overline{[3.4]}+\overline{\{3.4\}}=\overline{3}+\overline{0.4}=\overline{0}+\overline{0.4}$$
$$=\overline{0.4}$$

$\overline{6.4}=\overline{0.4}$，$\overline{-3.6}=\overline{0.4}$，即$\overline{3.4}=\overline{6.4}=\overline{-3.6}=\overline{0.4}$。

一般地，$\overline{x}=\overline{y}\Longleftrightarrow\{x\}=\{y\}$，从而$\overline{x}=\overline{\{x\}}$。

再如　$\overline{3.4}+\overline{6.4}=\overline{3.4+6.4}=\overline{9.8}=\overline{0.8}$，$\overline{6.4}+\overline{-3.6}=\overline{6.4+(-3.6)}=\overline{2.8}=\overline{0.8}$。

$4\,\overline{3.4}=\overline{4\times3.4}=\overline{13.6}=\overline{0.6}$，$4\,\overline{-3.6}=\overline{-14.4}=\overline{0.6}$。

此处因为$\overline{3.4}=\overline{-3.6}$，当然有$4\,\overline{3.4}=4\,\overline{-3.6}=4\,\overline{0.4}=\overline{0.6}$。这样

$$\eta: x\longmapsto\overline{x}=\overline{\{x\}}$$

就是使**Z**—模**Q**与其商模**Q**/**Z**同态的自然映射。

例3　设$M=Ra$为循环R—模。令

$$\varphi: r\longmapsto ra,\ \forall r\in R,$$

那么$R\overset{\varphi}{\sim}Ra$。而$\varphi$的核

$$ker\varphi=\{r\in R\mid ra=0\}.$$

即$ker\varphi$正是a在环R中的零化子$ann\,a$。于是

$$R/ker\varphi\overset{\bar{\varphi}}{\simeq}Ra\ 或\ R/ann\,a\overset{\bar{\varphi}}{\simeq}Ra,\quad \bar{\varphi}: \bar{k}\longmapsto ka.$$

例4　设环$R=M_2(\mathbf{Q})$，$N=\left\{\begin{pmatrix}a&o\\b&o\end{pmatrix}\middle|\ a,\ b\in\mathbf{Q}\right\}$是$R$—模$M=\{R;\ +\}$的子模。于是$N$是循环的：

$$N=Ra,\quad a=\begin{pmatrix}1&o\\o&o\end{pmatrix},\quad ann\,a=\left\{\begin{pmatrix}o&x\\o&y\end{pmatrix}\middle|\ x,\ y\in\mathbf{Q}\right\}.$$

则有

$$M\Big/ann\alpha\overset{\varphi}{\simeq}R\alpha,\quad \varphi:\overline{\begin{pmatrix}a&b\\c&d\end{pmatrix}}\longmapsto\begin{pmatrix}a&b\\c&d\end{pmatrix}\begin{pmatrix}1&0\\0&0\end{pmatrix}=\begin{pmatrix}a&0\\c&0\end{pmatrix}$$

另外也有 $N=R\beta$，$\beta=\begin{pmatrix}0&0\\1&0\end{pmatrix}$，$ann\beta=\left\{\begin{pmatrix}x&0\\y&0\end{pmatrix}\Big|\,x,\ y\in\mathbf{Q}\right\}$

于是

$$M\Big/ann\beta\overset{\psi}{\simeq}R\beta,\psi\ :\ \overline{\begin{pmatrix}a&b\\c&d\end{pmatrix}}\longmapsto\begin{pmatrix}a&b\\c&d\end{pmatrix}\begin{pmatrix}0&0\\1&0\end{pmatrix}=\begin{pmatrix}b&0\\d&0\end{pmatrix}.$$

显然 $ann\alpha\neq ann\beta$，但是有 $M\Big/ann\alpha\simeq M\Big/ann\beta$。

例5 设M，M'都是R—模，$\varphi:M\to M'$是R—同态．则有，

$$0\longrightarrow ker\varphi\overset{\tau}{\longrightarrow}M\overset{\eta}{\longrightarrow}M\Big/ker\varphi\longrightarrow 0,$$

与
$$0\longrightarrow Im\varphi\overset{\sigma}{\longrightarrow}M'\overset{\rho}{\longrightarrow}M'\Big/Im\varphi\longrightarrow 0$$

都是短正合列．此中，τ 与 σ 都是包含同态，η 与 ρ 都是自然同态。

以上讨论了 R—模M的商模概念的形成及其意义．我们的具体做法是从一个子模K出发，由它给 M划分成类(陪集)，以类为元素得到一个新的集合 M/K．而且按照自然的方法对M/K规定了类的加法和倍数乘法，把两个类相加就是通过类中元素相加；使R中元素去乘一个类就是该元素去乘类中的元素．这样便使M/K做成了R上的一个模—商模．同时，按如下的自然方式：

$$\eta:a\longmapsto\overline{a}=a+K,\quad\forall a\in M,$$

使得M/K是M的同态象，即

$$M\overset{\eta}{\sim}M/K.$$

而且η的核恰为当初的子模K：$ker\eta=K$。

下面我们将指出上述极其自然的过程的必然性．为此，我们需要如下的

定理2 设M是R—模，E是集合M上的一个等价关系，由E确定的商集合记作

$$M/E=\{\alpha/E \mid \alpha\in M\}$$

即

$$\alpha/E=\beta/E \Longleftrightarrow \alpha E\beta \text{或} (\alpha, \beta)\in E \quad ((\alpha, \beta)\in M^{(2)}).$$

而且M/E按

$$\alpha/E + \beta/E = \alpha+\beta/E$$

$$k\,\alpha/E=k\alpha/E, \ \forall k\in R, \alpha/E, \ \beta/E\in M/E$$

能够做成一个R—模，(或在映射

$$\eta: \alpha \longmapsto \alpha/E$$

之下，M/E是M的同态象，即$M\overset{\eta}{\sim}M/E$)
充分必要条件是M/E中存在一个元素M_E做成M的一个子模，使得

$$\alpha E\beta \Longleftrightarrow \alpha-\beta\in M_E.$$

从而M/E就是M关于子模M_E的商模M/M_E.

证 充分性是明显的，须要证明的只是必要性。

首先，令$0/E=M_E$，我们指出这个零元素所在的等价类正好是M的一个子模：

$\forall\ \alpha, \ \beta\in M_E, \ k\in R$,即$\alpha/E=\beta/E=0/E$,

$\Longrightarrow(\alpha+\beta)\big/E=\alpha/E+\beta/E=0/E+0/E=(0+0)\big/E=0/E$，即有$\alpha+\beta\in M_E$.

$\Longrightarrow k\alpha\big/E=k\ (\alpha/E)=k\ (0/E)=k0\big/E=0/E$, 即 $k\alpha\in M_E$. 从而，M_E是M的子模。

其次，如果$\alpha/E=\beta/E\Longrightarrow(\alpha-\beta)\big/E=\alpha/E-\beta/E=\alpha/E-\alpha/E=(\alpha-\alpha)\big/E=0/E$，即$\alpha-\beta\in M_E$. 反之，如果 $\alpha-\beta\in M_E\Longrightarrow\beta/E=\beta/E+0/E=\beta/E+(\alpha-\beta)\big/E=(\beta+(\alpha-\beta))\big/E=\alpha/E$. 这样，

必要性也被证明了. ▌

如果H_1，H_2都是R—模M的子模，当$H_1 \subsetneq H_2$时，则称H_2是在H_1之上的子模.

定理3 设M是R—模，K是M的子模. 令$L_K(M)=\{H \mid H$为M的子模，且$K \subseteq H\}$，$L(M/K)=\{\overline{H} \mid \overline{H}$是$M/K$的子模$\}$. 那么自然同态 $\eta: M \longrightarrow M/K$在$L_K(M)$与$L(M/K)$之间诱导出一个双射（也用$\eta$表示）：

$$\eta: H \longmapsto \eta(H), \ \forall H \in L_K(M),$$

而且保持包含关系不变，即$H_1 \subseteq H_2 \Longrightarrow \eta(H_1) \subseteq \eta(H_2)$.

证 首先，η是$L_K(M)$到$L(M/K)$的一个映射是明确的. 其次指出η是满射. $\forall \overline{H} \in L(M/K)$，则有$\overline{H}=\{\overline{\alpha}=\alpha+K \mid \alpha \in H \subseteq M\}$. 我们肯定这个$H$就是$M$的一个子模，且$\eta(H)=\overline{H}$. 事实上$\forall \alpha$，$\beta \in H$，$k \in R$，都有$\overline{\alpha+\beta}=\overline{\alpha}+\overline{\beta} \in \overline{H}$，从而$\alpha+\beta \in H$. $\overline{k\alpha}=k\overline{\alpha} \in \overline{H}$，从而$k\alpha \in H$. 所以，$H$是$M$的子模. 至于$\eta(H)=\overline{H}$，则是明显的.

再有，η也是单射. 若H_1，H_2均为M的子模，且$K \subseteq H_1$，$K \subseteq H_2$，又使$\eta(H_1)=\eta(H_2)$. 于是由于$\eta(H_1)=\{\overline{\alpha}=\alpha+K \mid \alpha \in H_1\}$，$\eta(H_2)=\{\overline{\beta}=\beta+K \mid \beta \in H_2\}$. 当$\eta(H_1)=\eta(H_2)$时，$\forall \alpha \in H_1$，必有某一个$\beta \in H_2$，使得$\overline{\alpha}=\overline{\beta}$. 从而$\alpha-\beta \in K$. 即有$\alpha=\beta+\gamma$，$\gamma \in K$，又因$K \subseteq H_2$，故而$\alpha=\beta+\gamma \in H_2$，亦即$H_1 \subseteq H_2$. 类似地，可知$H_2 \subseteq H_1$，这样，$H_1=H_2$. 总之，$\eta$在$L_K(M)$与$L(M/K)$之间来看是一个双射，而$\eta$保持子模的包含关系不变由上节定理1之推论即得. ▌

这个定理表明，商模M/K的每一个子模都可唯一的写成H/K的形式，其中H是M的一个在K之上的子模. 再有，如果我们注意到上节例10的结果，上面定理3的证明将是相当简明的.

例6 设$M=\{0, a, b, c\}$是klein四元群，于是M可以看成**Z**—模. 令$K=\{0, a\}$为M的一个子模，则有商模

$$M/K=\{\overline{0}, \overline{b}\}.$$

这样，M的在K之上的子模与M/K的子模之间成一一对应。虽然M共有五个子模，但在K之上的子模恰有两个，即

$$K=\{0,\ a\},\ M=\{0,\ a,\ b,\ c\}.$$

从而商模M/K的子模也恰有两个：$\{\overline{0}\}$，$\{\overline{0},\ \overline{b}\}$，此时$\{\overline{0}\}=K/K$，$\{\overline{0},\ \overline{b}\}=M/K$。

定理4 设M，M'是R—模，$\varphi: M\longrightarrow M'$是$R$—同态。令$N$，$N'$分别是$M$与$M'$的子模。那么映射

$$\overline{\varphi}: M/N\longrightarrow M'/N',$$

其中$\overline{\varphi}: \overline{\alpha}\longmapsto\overline{\varphi(\alpha)}$（即$\overline{\varphi}(\overline{\alpha})=\overline{\varphi(\alpha)}$或$\overline{\varphi}: \alpha+N\longmapsto\varphi(\alpha)+N'$）是$M/N$到$M'/N'$的$R$—同态$\Longleftrightarrow\varphi(N)\subseteq N'$。并且

（1）$\overline{\varphi}$是单同态$\Longleftrightarrow N=\varphi^{-1}(N')$。

（2）$\overline{\varphi}$是满同态$\Longleftrightarrow Im\varphi+N'=M'$。

证 先证充分性。设$\varphi(N)\subseteq N'$。我们指出$\overline{\varphi}$的合理性，即$\overline{\varphi}$的单值性。

若$\overline{\alpha}=\overline{\beta}\Longrightarrow\alpha-\beta\in N$，于是$\varphi(\alpha-\beta)\in N'$，从而$\varphi(\alpha)-\varphi(\beta)\in N'\Longrightarrow\overline{\varphi(\alpha)}=\overline{\varphi(\beta)}$。这就是$\overline{\varphi}$的单值性。下面说明$\overline{\varphi}$是$R$—同态。事实上

$$\overline{\varphi}(\overline{\alpha}+\overline{\beta})=\overline{\varphi}(\overline{\alpha+\beta})=\overline{\varphi(\alpha+\beta)}=\overline{\varphi(\alpha)+\varphi(\beta)}$$

$$=\overline{\varphi(\alpha)}+\overline{\varphi(\beta)}=\overline{\varphi}(\overline{\alpha})+\overline{\varphi}(\overline{\beta}).$$

$$\overline{\varphi}(k\overline{\alpha})=\overline{\varphi}(\overline{k\alpha})=\overline{\varphi(k\alpha)}=k\overline{\varphi(\alpha)}=k\overline{\varphi(\alpha)}=k\overline{\varphi}(\overline{\alpha}).$$

这就说明$\overline{\varphi}$确是M/N到M'/N'的一个R—同态。

再证必要性。若已知$\overline{\varphi}$是M/N到M'/N'的一个R—同态。则有$\overline{\varphi}(\overline{0})=\overline{0}$。于是$\forall\alpha\in N$，$\overline{\alpha}=\overline{0}\Longrightarrow\overline{\varphi(\alpha)}=\overline{\varphi}(\overline{\alpha})=\overline{\varphi}(\overline{0})=\overline{0}$，$\Longrightarrow\varphi(\alpha)\in N'$，$\varphi(N)\subseteq N'$。

最后，$\overline{\varphi}$是单同态$\Longleftrightarrow ker\,\overline{\varphi}=\{\overline{0}\}$。即$\overline{\varphi}(\overline{a})=\overline{0}$当且仅当$\overline{a}=\overline{0}$。亦即$\varphi(a)\in N'\Longleftrightarrow a\in N$。故而$\varphi^{-1}(N')=N$，即（1）成立。$\overline{\varphi}$是满同态$\Longleftrightarrow M'=\{\varphi(a)+N'\,|\,a\in M\}$，亦即。$Im\varphi+N'=M'$所以（2）成立。∎

定理5 （第一同构定理）设M，M'是R—模，$\varphi:M\longrightarrow M'$是$R$—满同态，即$M\overset{\varphi}{\sim}M'$，$ker\,\varphi=K$。令$N$为$M$的子模，且$K\subseteq N$，$\varphi(N)=N'$。那么映射

$$\overline{\varphi}:M/N\longrightarrow M'/N',\quad \overline{\varphi}:a+N\longmapsto\varphi(a)+N',$$

是一个R—同构，即$M/N\overset{\overline{\varphi}}{\simeq}M'/N'$。

证 显然，这是定理4的一个特殊情形。从而首先可以肯定映射$\overline{\varphi}$是M/N到M'/N'的一个R—同态。又因$\varphi(N)=N'$，即$N=\varphi^{-1}(N')$，所以$\overline{\varphi}$是单同态。并且φ是满同态，当然$Im\varphi+N'=M'$。从而$\overline{\varphi}$也是满同态。这样$\overline{\varphi}$就是一个R—同构。∎

推论 若M为R—模，K，N都是M的子模，且$K\subseteq N$。那么

$$M/N\simeq M/K\Big/N/K.$$

事实上 取$M/K=M'$时，这里就是定理5的特殊情形。

定理6 （第二同构定理）设M是R—模，N_1与N_2都是M的子模。那么商模$\boldsymbol{N}_1\Big/(\boldsymbol{N}_1\cap\boldsymbol{N}_2)$与$(\boldsymbol{N}_1+\boldsymbol{N}_2)\Big/\boldsymbol{N}_2$同构。

证 考虑M到$M/\boldsymbol{N}_2$的自然同态η。于是η在N_1上的限制

$$\eta':a\longmapsto\overline{a}=a+N_2,\quad\forall a\in N_1$$

是N_1到$(\boldsymbol{N}_1+\boldsymbol{N}_2)\Big/\boldsymbol{N}_2$的一个$R$—满同态。考察$\eta'$的核$ker\eta'$。若$a\in\boldsymbol{N}_1$，$a\in ker\,\eta'$，则有$\eta'(a)=\overline{0}$，即$a+\boldsymbol{N}_2=\boldsymbol{N}_2\Longrightarrow a\in\boldsymbol{N}_2$，从而$a\in\boldsymbol{N}_1\cap\boldsymbol{N}_2$。故而$ker\eta'=\boldsymbol{N}_1\cap\boldsymbol{N}_2$。由同态基本定理，即有

$$N_1\Big/(N_1\cap N_2)\overset{\overline{\eta'}}{\simeq}(N_1+N_2)/N_2,$$

其中$\overline{\eta'}$：$a+(N_1\cap N_2)\longmapsto a+N_2$. $\forall a\in N_1$. ∎

下面再介绍一个形式更为复杂的第三同构定理，来结束这一节的讨论。第三同构定理，通常也叫 *Zassenhous* 引理，它在下一节将被用到。

定理7 （第三同构定理）设M是R—模。H_1'，H_2' 与 H_1，H_2都是M的子模，且$H_1'\subseteq H_1$，$H_2'\subseteq H_2$。那么商模

$$H_1'+(H_1\cap H_2)\Big/H_1'+(H_1\cap H_2')\text{与}$$

$$H_2'+(H_1\cap H_2)\Big/H_2'+(H_1'\cap H_2)$$

同构。

证 因为 $H_1'\cap H_2\subseteq H_1\cap H_2$，那么

$$(H_1\cap H_2)+H_2'+(H_1'\cap H_2)=(H_1\cap H_2)+H_2'.$$

于是，由第三节的定理4，则有

$$(H_1\cap H_2)\cap[H_2'+(H_1'\cap H_2)]=(H_1\cap H_2)\cap H_2'$$
$$+(H_1'\cap H_2)=(H_1\cap H_2')+(H_1'\cap H_2)$$

这样，令$N_1=H_1\cap H_2$，$N_2=H_2'+(H_1'\cap H_2)$，由第二同构定理，则得

$$H_1\cap H_2\Big/(H_1\cap H_2')+(H_1'\cap H_2)$$

$$\simeq H_2'+(H_1\cap H_2)\Big/H_2'+(H_1'\cap H_2)\ .$$

同理，因为$H_1\cap H_2'\subseteq H_1\cap H_2$，那么

$$(H_1\cap H_2)+H_1'+(H_1\cap H_2')=H_1'+(H_1\cap H_2).$$

同样，根据第三节的定理4，则有

$$(H_1\cap H_2)\cap[H_1'+(H_1\cap H_2')]$$
$$=(H_1\cap H_2)\cap H_1'+(H_1\cap H_2')=(H_1'\cap H_2)+(H_1\cap H_2').$$

令$N_1=H_1\cap H_2$，$N_2=H_1'+(H_1\cap H_2')$，由第二同构定理，则

得

$$H_1\cap H_2\Big/(H_1'\cap H_2)+(H_1\cap H_2')$$

$$\simeq H_1'+(H_1\cap H_2)\Big/H_1'+(H_1\cap H_2')$$

从而得到

$$H_1'+(H_1\cap H_2)\Big/H_1'+(H_1\cap H_2')$$

$$\simeq H_2'+(H_1\cap H_2)\Big/H_2'+(H_1'\cap H_2).\ ▌$$

习　　题

1．设A，B都是R—模M的子模．证明，按自然的映射方法，如下的模同态序列都是正合列：

(1)　$0\longrightarrow A\cap B\longrightarrow B\longrightarrow B\big/A\cap B\longrightarrow 0$．

(2)　$0\longrightarrow A\cap B\longrightarrow A\longrightarrow A\big/A\cap B\longrightarrow 0$．

(3)　$0\longrightarrow A\big/A\cap B\longrightarrow M\big/B\longrightarrow M\big/A+B\longrightarrow 0$．

(4)　$0\longrightarrow B\big/A\cap B\longrightarrow M\big/A\longrightarrow M\big/A+B\longrightarrow 0$．

2．设R为主理想环，M为R上的循环模：$M=\langle a\rangle$．如果存在一个素元素p，使$\operatorname{ann}a=(p^k)$，那么

$M_0=M$，$M_1=pM$，$M_2=p^2M$，$\cdots$，　$M_{k-1}=p^{k-1}M$，

$M_k=p^kM=\{0\}$是M的全部子模．

3．设R为有恒等元素的交换环．令

$R_n[x]=\{a_0+a_1x+\cdots+a_nx^n\,|\,a_i\in R\}$．$n=0$，1，2，$\cdots$．

证明：

（1）$R_n[x]$（$n\geqslant 0$）均为R—模，并且

$$R_0=R\subseteq R_1[x]\subseteq R_2[x]\subseteq\cdots\subseteq R_{n-1}[x]\subseteq R_n[x].$$

（2）对$n\geqslant 1$，$R_{n-1}[x]\simeq R_n[x]\Big/R$.

4. 设R为有恒等元素，没有零因子的交换环．证明：

（1）对任一非零元素 $x\in R$，$Rx^n=\{yx^n|y\in R\}$ 均为模 R 的子模，并且$R\supseteq Rx\supseteq Rx^2\supseteq\cdots\supseteq Rx^{n-1}\supseteq Rx^n\supseteq\cdots$.

（2）$Rx^{n-1}\Big/Rx^n\simeq R\Big/Rx$，$n=1, 2, \cdots$.

5. 设A，B，C都是R—模，$\sigma: A\longrightarrow B$，$\tau: B\longrightarrow C$为$R$—同态．证明，模同态序列

$$0\longrightarrow \ker\sigma\longrightarrow \ker\tau\sigma\longrightarrow \ker\tau\longrightarrow B\Big/Im\sigma\longrightarrow C\Big/Im\tau\sigma\longrightarrow$$

$C\Big/Im\tau\longrightarrow 0$ 是正合列．

6. 设A，B都是R—模，$\sigma: A\longrightarrow B$是$R$—同态．证明：

（1）σ 是单同态$\Longleftrightarrow$对任二R—同态，τ_1，$\tau_2: C\longrightarrow A$，如果 $\sigma\tau_1=\sigma\tau_2$，则必有$\tau_1=\tau_2$.

（2）σ 是满同态$\Longleftrightarrow$对任二R—同态，ρ_1，$\rho_2: B\longrightarrow D$，如果 $\rho_1\sigma=\rho_2\sigma$，则必有$\rho_1=\rho_2$.

7. 设M为R—模，I 为R的左理想．证明：

（1）对任一非空子集$S\subseteq M$，子集$IS=\left\{\sum_{i=1}^{n}r_i\alpha_i\,\middle|\,r_i\in I,\ \alpha_i\in S\right\}$是$M$的子模．

（2）如果 I 是R的真理想，那么取

$$\bar{r}\,\bar{\alpha}=\overline{r\alpha}\quad (\text{即}(r+I)(\alpha+IM)=r\alpha+IM)$$

为倍数乘法，则使商集M/IM做成商环R/I上的模．

§6 单模 Jordan—Hölder 定理

我们都已知道，由一个元素生成的模—循环模 $M=Ra$ 是非常简单的一种模，它的结构由它的生成元素的零化子所刻划。但是，还有比一般循环模更为简单的模，即所谓的单模，本节介绍单模的概念及其基本性质。进而证明一个定理，即 *Jordan—Hölder* 定理，它表明对某些模可以逐次划分成有限个单模去加以研究。

定义1 设M为R—模，$M\neq\{0\}$。如果M没有非平凡的子模，即除了$\{0\}$、M之外，M再没有其它的子模，则称M是单模。

例1 令M为域F上的线性空间，那么，M是单模$\Longleftrightarrow \dim M=1$。

例2 整数加法群$\mathbf{Z}$做为$\mathbf{Z}$—模不是单模；$\mathbf{Z}_n$做为$\mathbf{Z}$—模是单模$\Longleftrightarrow n$为素数。

例3 若R—模M是单模，那么M一定是循环模，反之则未必。

事实上 若M是单模，则$M\neq\{0\}$，任取M的一个非零元素a，$N=Ra$是M的一个子模，因为$a\in N$，所以$N\neq\{0\}$，从而$N=M$，即$M=Ra$，是循环模，反之，由例2便可得知。

例4 令环$R=M_3(\mathbf{Q})$，把R看成R—模，显然不是单模。再如

$$N_1=\left\{\begin{pmatrix}a_1 & a_2 & 0\\ b_1 & b_2 & 0\\ c_1 & c_2 & 0\end{pmatrix}\middle| a_i,\ b_i,\ c_i\in\mathbf{Q}\right\}\text{看成}R\text{—模也不是单模。}$$

$$N_2=\left\{\left(\begin{array}{ccc}a&0&0\\b&0&0\\c&0&0\end{array}\right)\middle|\, a,\ b,\ c\in\mathbf{Q}\right\}$$ 看成R—模则是单模.

但是，N_2也可以看成$\mathbf{Q}$上的模，这时N_2就不是$\mathbf{Q}$上的单模了.

定理1 设M是R—模. 以下条件是等价的：

（1）M是单模.

（2）M是循环模，而且任一非零元素都是生成元素.

（3）$M\simeq R/I$，I是R的一个极大左理想，即I是真左理想，且不存在左理想J，使$I\subset J\subset M$.

证 （1）$\Longrightarrow$（2）若M是单模，$\forall a\in M$，$a\neq 0$. $\Longrightarrow$ $N=Ra$是M的子模，且$N\neq\{0\}\Longrightarrow N=M$，即$\forall a\in M$，$a\neq 0$都有$M=Ra$.

（2）$\Longrightarrow$（3）若M是循环模，每一个非零元素都是生成元. 于是，$\forall a\in M$，$a\neq 0$，则有

$$M=Ra\overset{\varphi}{\simeq}R/I,\quad I=\operatorname{ann}a$$

我们指出，I是极大的左理想，令J是R的一个左理想，使$I\subset J$. 去证$J=R$即可. 任取$b\in J$，$b\overline{\in}I$，则有$\beta\in M$，$\beta\neq 0$，使

$$\varphi:\beta\longmapsto\overline{b}$$

于是，由$M=R\beta\Longrightarrow R/I=\{r\overline{b}\mid r\in R\}\Longrightarrow\forall x\in R$，存在$r\in R$使$x=rb+a$，$a\in I$，因为$I\subset J$，$a\in J\Longrightarrow x\in J$. 从而$J=R$.

（3）$\Longrightarrow$（1）若$M\simeq R/I$，而I是R的极大左理想. 由此可知，在I与R之间，除了I，R之外，再没有左理想. 从而，在$\{\overline{0}\}$与R/I之间，除了$\{\overline{0}\}$，R/I之外，再没有R/I的子模，即，R/I是R上的单模. 亦即M是R上的单模. ▌

定理2 设M，N都是R—模，$\sigma: M\longrightarrow N$是一个非零的$R$—同态. 那么

（1）若M是单模，则σ是单同态.

（2）若N是单模，则σ是满同态。

证 因为M是单模，所以 $ker\sigma=\{0\}$或$ker\sigma=M$。由于σ是非零的，从而 $ker\sigma=\{0\}$。即，σ 是单同态，（1）成立。

如果N是单模，则有 $Im\sigma=\{0\}$ 或 $Im\sigma=N$。因为σ是非零的，所以 $Im\sigma=N$。即σ是满同态，（2）成立。▌

定理3 （Schur）若R—模M是单模，那么End_RM是除环。

证 只须指出 End_RM的非零元素皆有逆就行了。而 End_RM 的非零元素都是单模M的自同态。于是，由定理2，M的每一个非零自同态σ既是单的又是满的，从而，σ是可逆的。亦即 End_RM是一个除环。▌

我们已经看到，一个 R—模 M，如果是单模，那么它的性质和结构都是特别简单的。当M本身不是单模时，一般地，它一定包含有非平凡的子模。于是，可以考虑如下的一个子模的序列：

$$M=M_1\supset M_2\supset M_3\supset\cdots\supset M_r\supset M_{r+1}=\{0\}.$$

从而得到一个商模序列：

$$\overline{M}_1=M_1/M_2,\quad \overline{M}_2=M_2/M_3,\quad \cdots,\quad \overline{M}_r=M_r\Big/M_{r+1}$$

使得

$$M=M_1\sim M_1/M_2,\ M_2\sim M_2/M_3,\ \cdots,\ M_r\sim M_r\Big/M_{r+1},$$

这样，通过对这一串商模的研究，对于认识和揭示原来的模M的性质和结构，无疑是有益的。尤其是，当这一串商模，每一个都是单模时，这种考虑自然就更是有效的。下面我们就来讨论这样的问题。

定义2 设M是R—模，称M的一个真降的子模序列：

$$T: M=M_1\supset M_2\supset M_3\supset\cdots\supset M_r\supset M_{r+1}=\{0\}$$

为M的一个子模塔。并把商模序列：

$$M_1/M_2,\ M_2/M_3,\ \cdots,\ M_r\Big/M_{r+1}$$

叫做这个子模塔的**商序列**，此中商模的个数r叫做塔T的高，记

作$h(T)$。特别地，当商序列中每一商模都是单模时，则称子模塔T为Jordan—Hölder 塔。

定义3 设M为R—模 M的两个子模塔

$$T_1: M=M_1\supset M_2\supset M_3\supset\cdots\supset M_r\supset M_{r+1}=\{0\}.$$

$$T_2: M=N_1\supset N_2\supset N_2\supset\cdots\supset N_r\supset N_{r+1}=\{0\}.$$

如果 T_1 的商序列 $\overline{M}_1=M_1/M_2$，$\overline{M}_2=M_2/M_3$，…，$\overline{M}_r=M_r\big/M_{r+1}$中之商模，在适当调正顺序之后能与$T_2$的商序列中之商模依次是同构的，即

$$\overline{M}_{i_1}\simeq N_1/N_2,\ \overline{M}_{i_2}\simeq N_2/N_3,\ \cdots,\ \overline{M}_{i_r}\simeq N_r\big/N_{r+1},$$

则称子模塔T_1与T_2是等价的。此中 i_1，i_2，…，i_r 是 1，2，…，r 的一个适当的排列。

显然，等价的两个子模塔必有相同的高。

定义4 设M为R—模，M的两个子模塔

$$T: M=M_1\supset M_2\supset M_3\supset\cdots\supset M_r\supset M_{r+1}=\{0\},$$

$$S: M=N_1\supset N_2\supset N_3\supset\cdots\supset N_s\supset N_{s+1}=\{0\},$$

如果子模塔T中的子模都在子模塔S中出现，则称 S 是T的加细。

下面通过一些例子来具体的熟悉上面的概念。

例5 令$M=\mathbf{Z}_6$，做为$\mathbf{Z}$—模。$N=\{\overline{0},\overline{3}\}$，$P=\{\overline{0},\overline{2},\overline{4}\}$，于是

$$T: M\supset N\supset\{\overline{0}\};\ S: M\supset P\supset\{\overline{0}\}.$$

是M的两个子模塔，高都等于 2 。它们的商序列分别是

$$M/N,\ N\big/\{\overline{0}\}\ 与\ M/P,\ P\big/\{\overline{0}\},$$

把T的商序列 M/N，$N\big/\{\overline{0}\}$ 调正一下顺序：$N\big/\{\overline{0}\}$，M/N，则有

$$N\big/\{\overline{0}\}\simeq M/P,\quad M/N\simeq P\big/\{\overline{0}\}.$$

从而，Z_6 的这两个子模塔是等价的．并且容易知道，T 与 S 都是Jordan—Hölder 塔．

例6　令$M=\mathbf{Z}$，看做$\mathbf{Z}$—模．于是

$T_1:\mathbf{Z}\supset\langle 2\rangle\supset\{0\}$，

$T_2:\mathbf{Z}\supset\langle 2\rangle\supset\langle 4\rangle\supset\{0\}$，

$T_3:\mathbf{Z}\supset\langle 2\rangle\supset\langle 4\rangle\supset\langle 8\rangle\supset\{0\}$，

都是$\mathbf{Z}$的子模塔，而且T_3是T_2的加细，T_2是T_1 的加细，容易看出，T_1，T_2，T_3都不是 Jordan—Hölder 塔．其实，$\mathbf{Z}$根本不存在 Jordan—Hölder塔，这是因为，对 $\mathbf{Z}$的任一非零子模N，必有子模N'，使$N\supset N'\supset\{0\}$．由此便可断言，$\mathbf{Z}$ 没有 Jordan—Hölaer 塔．

例7　考虑域 F上的 n 维线性空间 V．任取 V 的一个基 e_1，e_2，…，e_n．于是，V有子模塔

$$T:V=\langle e_1,\ e_2,\ \cdots,\ e_n\rangle\supset\langle e_1,\ e_2,\ \cdots,\ e_{n-1}\rangle\supset\cdots\supset\langle e_1,\ e_2\rangle\supset\langle e_1\rangle\supset\{0\},$$

容易看出T是一个 Jordan—Hölder 塔，且有 $h(T)=n=dimV$．

如果取无限维空间$V=F[x]=\{a_0+a_1x+\cdots+a_nx^n\,|\,a_i\in F\}$，于是 V有子模塔

$$T_1:V\supset\langle 1,\ x,\ \cdots,\ x^m\rangle\supset\langle 1,\ x,\ \cdots,\ x^{m-1}\rangle\supset\cdots\supset\langle 1,\ x\rangle\supset\langle 1\rangle\supset\{0\},$$

$$T_2:V\supset\langle x,\ x^2,\ \cdots\rangle\supset\langle x^2,\ x^3,\ \cdots\rangle\supset\cdots\supset\langle x^m,\ x^{m+1},\ \cdots\rangle\supset\{0\}$$

都是V的子模塔，容易看出，二者都不是Jordan—Hölder 塔．并且不难指出，模$V=F[x]$ 不存在 Jordan—Hölder 塔（怎么解释？）．

例8　设M为任一R—模．那么子模塔

$$T:M=M_1\supset M_2\supset M_3\supset\cdots\supset M_r\supset M_{r+1}=\{0\}$$

是 Jordan—Hölder 塔$\Longleftrightarrow\forall_i$，$M_{i+1}$在$M_i$中看，是 M_i 的极大子模，即不存在M_i的子模（当然也是 M的子模）N，使 $M_i\supset N$

$\supset M_{i+1}$.

事实上 由子模的对应定理（§5定理3），适合关系 $M_i \supset N \supset M_{i+1}$ 的子模N与商模 M_i/M_{i+1} 的子模是一一对应的。这样，M_i/M_{i+1} 是单模$\Longleftrightarrow M_i/M_{i+1}$ 没有非平凡的子模$\Longleftrightarrow$在M_i与M_{i+1}之间没有异于M_i，M_{i+1}的子模。故而，子模塔T是 Jordan—Hölder 塔$\Longleftrightarrow M_{i+1}$在$M_i$中看是极大子模。

显然，模M的任一Jordan—Hölder 塔T不能再加细为不同于T的子模塔。换句话说，模M的 Jordan—Hölder塔任意加细得到的子模塔还是原来的子模塔。

定理4 （*Schreier* 加细定理）设M为R—模，T_1，T_2是M的两个子模塔

$$T_1: M = M_1 \supset M_2 \supset M_3 \supset \cdots \supset M_r \supset M_{r+1} = \{0\},$$

$$T_2: M = M'_1 \supset M'_2 \supset M'_3 \supset \cdots \supset M'_s \supset M'_{s+1} = \{0\}.$$

那么可以把T_1加细成子模塔S_1；把T_2加细成子模塔S_2，使得S_1与S_2等价。

证 我们用第三同构定理，即 Zassenhous 引理，来证明这个加细定理。

对任一 $i=1, 2, \cdots, r$，令

$$M_{i+1,j} = M_{i+1} + (M_i \cap M'_j),\ j=1, 2, \cdots, s, s+1,$$

对任一$j=1, 2, \cdots, s$，令

$$M'_{j+1,i} = M'_{j+1} + (M'_j \cap M_i),\ i=1, 2, \cdots, r, r+1.$$

特别地，有

$$M_{i+1,1} = M_{i+1} + (M_i \cap M'_1) = M_{i+1} + (M_i \cap M) = M_{i+1} + M_i = M_i,$$

$$M_{i+1,s+1} = M_{i+1} + (M_i \cap M'_{s+1}) = M_{i+1} + (M_i \cap \{0\}) = M_{i+1} + \{0\} = M_{i+1}$$

不失一般性，可以认为 $s \leqslant r$。这时，对 $k=s+2, \cdots, r$ 规定：

$$M_{i+1,k} = M_{i+1,s+1}.$$

这样，得到如下的两个子模序列：

$$T'_1: M\supset\cdots\supset M_i=M_{i+1,1}\supseteq\cdots\supseteq M_{i+1,s+1}=\cdots$$
$$=M_{i+1,r+1}=M_{i+1}\supset\cdots\supset\{0\},$$
$$T'_2: M\supset\cdots\supset M'_j=M'_{j+1,1}\supseteq\cdots\supseteq M'_{j+1,r+1}=$$
$$=M'_{j+1,r+1}=M'_{j+1}\supset\cdots\supset\{0\}.$$

考察T'_1、T'_2中相邻的两个子模：

$$M_{i+1,j}=M_{i+1}+(M_i\cap M'_j)\text{ 与}$$
$$M_{i+1,j+1}=M_{i+1}+(M_i\cap M'_{j+1}),$$
$$M'_{j+1,i}=M'_{j+1}+(M'_j\cap M_i)\text{ 与}$$
$$M'_{j+1,i+1}=M'_{j+1}+(M'_j\cap M_{i+1}).$$

由 *Zassenhous* 引理，则有

$$M_{i+1,j}\Big/M_{i+1,j+1}\simeq M'_{j+1,i}\Big/M'_{j+1,i+1}.$$

由此可知，在子模序列T'_1与T'_2中，对重复出现的相同子模只留下一个，这样得到的两个子模序列S_1与S_2分别是在T_1与T_2基础上加细而成的子模塔，并且S_1与S_2是等价的。■

定理5 （*Jordan—Hölder* 定理）R—模M的任二*Jordan—Hölder* 塔

$$T_1: M=M_1\supset M_2\supset M_3\supset\cdots\supset M_r\supset M_{r+1}=\{0\},$$
$$T_2: M=M'_1\supset M'_2\supset M'_3\supset\cdots\supset M'_s\supset M'_{s+1}=\{0\}.$$

是等价的。特别地，$r=s$ 即M的任二*Jordan—Hölder* 塔的高相同。

证 由 *Schreier* 加细定理，可以把T_1，T_2加细成子模塔S_1与S_2，使S_1与S_2等价，但是T_1，T_2都是*Jordan—Hölder*塔，而*Jordan—Hölder* 塔的任意加细得到的子模塔必定还是原来的塔。这样，S_1就是T_1，S_2就是T_2。亦即T_1与T_2是等价的。由此自然有 $r=s$。■

定义5 如果R—模M有高为r的*Jordan—Hölder* 塔，则称M为有限高的。r叫做模M的高，记作 $h(M)=r$。为了方便，零模算做有限高的，并约定其高为0。

命题1 如果R—模M是有限高的那么M的任一子模塔T均可加细成为Jordan—Höldaer 塔，从而 $h(T)\leqslant h(M)$。并且 $h(T)=h(M)\Longleftrightarrow T$ 本身就是Jordan—Hölder 塔。

证 任取M的一个 Jordan—Hölder 塔

$$T: M=M_0\supset M_1\supset M_2\supset M_3\supset\cdots\supset M_r\supset M_{r+1}=\{0\}.$$

令

$$S: M=N_1\supset N_2\supset N_3\supset\cdots\supset N_s\supset N_{s+1}=\{0\}$$

为M的任一子模塔，于是，S可加细成一个子模塔S'，使S'与T等价。而与 Jordan—Hölder 塔等价的子模塔自然也是 Jordan—Hölder 塔。所以，S'是 Jordan—Hölder 塔，并且$h(S)\leqslant h(S')=r$。即 $h(S)\leqslant h(M)$ 。最后，如果 $h(S)=h(M)$，这说明子模塔S不须要再加细就已经是 Jordan—Hölder 塔了。从而，S是 Jordan—Hölder 塔$\Longleftrightarrow h(S)=h(M)$。▌

命题2 如果R—模M是有限高的，那么M的任一子模N也是有限高的，且 $h(N)\leqslant h(M)$。进而 $h(N)=h(M)\Longleftrightarrow N=M$。

证 对于M的任一非平凡子模N，则有子模塔$M\supset N\supset\{0\}$。于是，把这个子模塔加细成一个 Jordan—Hölder 塔：

$$M=M_1\supset\cdots\supset N\supset N_1\supset\cdots\supset N_s\supset\{0\},$$

顺便就得到子模N的一个 Jordan—Hölder塔。

$$N\supset N_1\supset\cdots\supset N_s\supset\{0\}.$$

这就说明子模N是有限高的，而且 $h(N)\leqslant h(M)$。同时可以看出，当N是M的真子模时：$M\supset N$，必有 $h(N)<h(M)$。所以，$h(N)=h(M)\Longleftrightarrow N=M$。▌

命题3 设V是域F上的线性空间。那么，做为F—模，V是有限高的$\Longleftrightarrow V$是有限维空间，且 $\dim V=h(V)$。

证 如果V是有限维空间，$\dim V=n$。令$e_1, e_2, \cdots, e_n$是V的一个基底。于是有子模塔

$$T: V=V_1\supset\langle e_1, e_2, \cdots, e_{n-1}\rangle\supset\langle e_1, e_2, \cdots, e_{n-2}\rangle\supset\cdots\supset\langle e_1\rangle\supset\{0\}.$$

容易指出，T是一个 Jordan—Hölder 塔，且

$h(T)=n$。这就是说，V是有限高的，且 $h(V)=n=dimV$。

反之，如果V是有限高的，$h(V)=n$。那么，V中不会有多于 n 个的线性无关向量，不然，V将有高于 n 的子模塔存在，这是不可能的。从而V必是有限维空间，而且它的维数不能小于 n，因为不然，V的高将低于 n。这样，V是有限维空间，且 $dimV=h(V)$。▌

习　　题

1．证明：R—模M是单的$\Longleftrightarrow h(M)=1$．

2．设R—模M是有限高的。证明：对于M的任一子模N，都有一个 Jordan—Hölder 塔

$$T: M=M_1\supset M_2\supset M_3\supset\cdots\supset M_n\supset M_{n+1}=\{0\},$$

使N是T中的一项，即有 k，使$M_k=N$。

3．设M是有限高的R—模。证明：M的每一个子模N及商模M/N也都是有限高的，并且

$$h(N)+h(M/N)=h(M),$$

从而得出，$N=M\Longleftrightarrow h(N)=h(M)$。

4．设M，N都是R—模，其中M是有限高的，证明：如果 $\sigma: M\longrightarrow N$是$R$—同态，那么，$I_m\sigma$及$ker\sigma$都是有限高的，并且 $h(ker\sigma)+h(I_m\sigma)=h(M)$。

5．设M是有限高的R—模。A，B为M的任二子模。证明：

（1）$h(A+B)+h(A\cap B)=h(A)+h(B)$，

（2）$h(M/A+B)+h(M/A\cap B)=h(M/A)+h(M/B)$。

6．设M为有限高的R—模。证明：对于M的任一R—自同态 σ，都有

σ 是单同态$\Longleftrightarrow\sigma$ 是满同态。

7. 设M_1，M_2，…，M_n都是有限高的R—模。证明：如果存在一个正合列：

$$0 \longrightarrow M_1 \xrightarrow{\sigma_1} M_2 \xrightarrow{\sigma_2} \cdots \longrightarrow M_{n-1} \xrightarrow{\sigma_{n-1}} M_n \longrightarrow 0,$$

那么 $\sum_{r=1}^{n}(-1)^r h(M_r)=0$。

8. 本节定理 3 的逆是否成立？即，如果自同态环$End_R M$是除环，是否R—模M一定是单模？

9. 设R—模M，N都是有限高的。证明：如果存在R一同态$\sigma: M\longrightarrow N$，那么存在Jordan—Hölder 塔：

$$M=M_1\supset M_2\supset M_3\supset\cdots\supset M_r\supset M_{r+1}=\{0\},$$

$$N=N_1\supset N_2\supset N_3\supset\cdots\supset N_s\supset N_{s+1}=\{0\},$$

其中必有某个 i 与 j，使得

$$M_i/M_{i+1}\simeq N_j/N_{j+1}.$$

10. 利用 Jordan—Hölder 定理，证明算术基本定理：每一个大于1的正整数m都可写成素数的积：$m=p_1p_2\cdots p_s$，$p_i(i=1, 2,\cdots,s)$ 均为素数，并且在不计顺序的情况下，这种写法是唯一的。

§7 链 条 件

上一节讨论了模M的子模塔的一些基本性质。特别是，在模M存在 Jordan—Hölder 塔的前提下，得出有限高模的若干重要性质。这些性质对特殊的模—域 F 上的有限维线性空间来说，模的高和空间的维数是完全一致的。然而到目前为止，除了域F上的有限维线性空间这种极其特殊的模之外，对一般的 R—模 M 是否存在 Jordan—Hölder 塔，或者说M是否有限高的，还没有什么标准予以判断。为此，本节就来讨论这个问题，给出 R—模M是有限高的充分必要条件。

升链条件 设M为 R—模。如果不存在无限的、真升的子模序列：

$$M_1\subset M_2\subset M_3\subset\cdots\subset M_k\subset\cdots,$$

其中M_i均为M的子模，则称模M满足子模的升链条件。

换句话说，对模M的子模的任意一个递升序列：

$$M_1\subseteq M_2\subseteq M_3\subseteq\cdots\subseteq M_k\subseteq\cdots,$$

必存在 k，使得$M_k=M_{k+1}=\cdots$，就说模M满足子模的升链条件。

降链条件 设M为R—模。如果不存在无限的、真降的子模序列：

$$M_1\supset M_2\supset M_3\supset\cdots\supset M_k\supset\cdots,$$

其中M_i均为M的子模，则称模M满足子模的降链条件。

换句话说，对模M的子模的任意一个递降序列：

$$M_1\supseteq M_2\supseteq M_3\supseteq\cdots\supseteq M_k\supseteq\cdots,$$

必存在 k，使得 $M_k=M_{k+1}=\cdots$，就说模 M 满足子模的降链条件。

满足升链条件的模叫做诺特（*Noether*）模．满足降链条件的模叫做阿丁（*Artin*）模．

和上述两个链条件密切相关的，还有所谓的关于子模的极大条件和极小条件．

极大条件　设M为R—模．S为M之子模的任一非空集合，那么S中必有子模N，使得S中的任何子模P，如果$P\supseteq N$则$N=P$．这样，则称M满足子模的极大条件．上述之子模N叫做S中的一个极大子模．

换句话说，M之子模的任一非空集合S中必有子模N，使S中不存在真包含这个子模N的子模P，这时就说模M满足子模的极大条件．

极小条件　设M为R—模．S为M之子模的任一非空集合，那么S中必有子模N，使得S中的任何子模P，如果$P\subseteq N$，则$P=N$．这样，则称模M满足子模的极小条件．上述之子模N叫做S中的一个极小子模．

换句话说，M之子模的任一非空集合S中必有子模N，使S中不存在真含于这个子模N的子模P，这时就说模M满足子模的极小条件．

例1　设V是域F上的线性空间．那么下列条件是等价的：

（1）V是有限维空间，

（2）V满足子空间的升链条件和降链条件，

（3）V满足子空间的极大条件和极小条件．

证　(1)$\Longleftrightarrow$(2)，首先，(1)$\Longrightarrow$(2)是明显的．其次，用反证法可得(2)$\Longrightarrow$(1)．事实上，如果V是无限维空间，那么在V中存在一组向量：

$$e_1,\ e_2,\ \cdots,\ e_n,\ \cdots$$

其中任意有限个向量都是线性无关的，于是有子空间的两个链：

$$\langle e_1\rangle\subset\langle e_1,\ e_2\rangle\subset\cdots\subset\langle e_1,\ e_2,\ \cdots,\ e_n\rangle\subset\cdots,$$

$$\langle e_1,\ e_2,\ \cdots,\ e_n,\ \cdots\rangle\supset\langle e_2,\ e_3,\ \cdots,\ e_n,\ \cdots\rangle\supset\cdots\supset$$

$\langle e_n, e_{n+1}, \cdots\rangle \supset \cdots$,

前者是一个无限的真升的子空间链；后者是无限的真降的子空间链，这样，V不满足子空间的升链条件，也不满足子空间的降链条件。故得（1）$\Longleftrightarrow$(2)。

再证（1）$\Longleftrightarrow$(3) 首先，（1）$\Longrightarrow$(3) 也是显然的。其次，用反证法，把上面两个链的子空间分别做成两个子空间的集合S_1与S_2。明显可见，S_1中没有极大子空间，S_2中没有极小子空间。从而V既不满足极大条件，也不满足极小条件。即有（3）$\Longrightarrow$(1) 成立。

例2 令$M=\mathbf{Z}$，做为$\mathbf{Z}$—模，那么M满足子模的升链条件，但不满足降链条件，即M是诺特模，但不是阿丁模，同时不难指出，M满足子模的极大条件，但不满足极小条件。

例3 p 为取定的素数，令

$$M=\left\{\frac{m}{pk}\,\middle|\, m\in\mathbf{Z},\ k \text{ 为任意非负整数}\right\}.$$

易知M是一个加法群，从而M可看成$\mathbf{Z}$—模。于是，M有一个无限的，真升的子模链：

$$\mathbf{Z}\subset\mathbf{Z}\left(\frac{1}{p}\right)\subset\mathbf{Z}\left(\frac{1}{p^2}\right)\subset\cdots\subset\mathbf{Z}\left(\frac{1}{p^k}\right)\subset\mathbf{Z}\left(\frac{1}{p^{k+1}}\right)\subset\cdots.$$

其中$\mathbf{Z}\left(\frac{1}{p^k}\right)$表示由$\mathbf{Z}$和$\frac{1}{p^k}$生成的子模；$\mathbf{Z}\left(\frac{1}{p^k}\right)=\langle\mathbf{Z},\frac{1}{p^k}\rangle$.

这样，M不满足子模的升链条件，即M不是诺特模。又因为$\mathbf{Z}\subseteq M$，所以M也不满足子模的降链条件，即M也不是阿丁模。

例4 为了得到一个阿丁模M，但M不是诺特模的具体例子，我们进一步考察例3中的$\mathbf{Z}$—模M。

首先指出，$\mathbf{Z}\left(\frac{1}{p^k}\right)$是模$M$的在$\mathbf{Z}$之上的全部真子模（$k=0$，1，2，…）。为此，令$N$是$M$的在$\mathbf{Z}$之上的任一真子模。于是，必存在$k$，使

$$\mathbf{Z}\left(\frac{1}{p^k}\right)\subseteq N,\ \text{但}\mathbf{Z}\left(\frac{1}{p^{k+1}}\right)\nsubseteq N.$$

则必有$N=\mathbf{Z}\left(\frac{1}{p^k}\right)$，不然，令 $\alpha\in N$，$\alpha=\frac{m}{p^{k+l}}$，$(mp,)=1$，

$l\geqslant 1$。从而

$$\Longrightarrow\beta=p^{l-1}\alpha=\frac{m}{p^{k+1}}\in N。\text{令 } sp+tm=1,$$

$$\Longrightarrow\frac{1}{p^{k+1}}=\frac{sp+tm}{p^{k+1}}=\frac{s}{p^k}+t\frac{m}{p^{k+1}},\ \Longrightarrow\frac{1}{p^{k+1}}\in N$$

$$\Longrightarrow\mathbf{Z}\left(\frac{1}{p^{k+1}}\right)\subseteq N。$$这个矛盾肯定了$N=\mathbf{Z}\left(\frac{1}{p^k}\right)$.

这样，对商模$M/\mathbf{Z}$来说，由子模的对应定理，下列子模：

$$\mathbf{Z}/\mathbf{Z}=\{\overline{0}\}\subset\mathbf{Z}\left(\frac{1}{p}\right)\Big/\mathbf{Z}\subset\mathbf{Z}\left(\frac{1}{p^2}\right)\Big/\mathbf{Z}\subset\cdots\subset\mathbf{Z}\left(\frac{1}{p^k}\right)\Big/\mathbf{Z}\subset\cdots$$

恰是商模$M/\mathbf{Z}$的全部子模，由此可见，$M/\mathbf{Z}$ 是阿丁模，但不是诺特模。

例5 任一有限加法群 M，做为 $\mathbf{Z}$—模是诺特模，也是阿丁模。

下面给出链条件的一些基本性质。

命题1 设M为R—模．那么

（1）M满足子模的升链条件$\Longleftrightarrow M$满足子模的极大条件．

（2）M满足子模的降链条件$\Longleftrightarrow M$满足子模的极小条件．

证 先证（1）成立．如果M满足升链条件，令S是M之子模的任一非空集合．于是可以任取$M_1\in S$，若M_1不是S中的极大子模，则有子模 $M_2\in S$，使$M_1\subset M_2$．若 M_2 也不是 S 中的极大子模，则有$M_3\in S$，使$M_1\subset M_2\subset M_3$，由于$M$满足子模的升链条件，上边的做法不可能无限的进行下去．这样，当进行到某一步时（比如是第n步），必有子模$M_n\in S$，使得 S 中再没有真包

含M_n的子模。即S中有极大子模，M满足子模的极大条件。反之，如果M满足子模的极大条件，那么M一定不会有子模的无限，真升的序列。不然，这样一个序列中的子模做成的子模集合S将没有极大元素。故而M满足子模的升链条件。

（2）的证明与（1）完全类似，故而略去。▌

命题2 如果R—模M满足升（降）链条件，那么M的任一子模及商模也都满足升（降）链条件。

证 对M的任一子模N来说，N的子模自然也是M的子模。从而，当M满足升(降)链条件时，子模N必自然的满足升(降)链条件。

而对商模M/N来说，通过自然R—同态映射 η：$M\overset{\eta}{\sim}M/N$来看，M/N的子模与M的在N之上的子模是一一对应的，并且保持包含关系不变。从此便可明显看出，当M满足子模的升（降）链条件时，商模M/N也满足子模的升（降）链条件。▌

命题3 设M为R—模。如果M有某一个子模N，使N及M/N同时满足子模的升(降)链条件。那么模M也满足子模的升（降）链条件。

证 由于关于降链的情形与升链的情形是完全类似的。所以我们只对升链的情形给出证明。

设 $M_1\subseteq M_2\subseteq M_3\subseteq\cdots\subseteq M_r\subseteq\cdots$

是模M的任意一个子模的升链。去证存在 l，使

$$M_l=M_{l+1}=\cdots。$$

由M的这个子模升链，相应的得出以下两个升链：

$$M_1\cap N\subseteq M_2\cap N\subseteq\cdots\subseteq M_r\cap N\subseteq\cdots。$$

$$\eta(M_1)\subseteq\eta(M_2)\subseteq\eta(M_3)\subseteq\cdots\subseteq\eta(M_r)\subseteq\cdots。$$

其中η是M到M/N的自然同态。

因为N与M/N都满足子模的升链条件，于是

存在 n，使得$M_n\cap N=M_{n+1}\cap N=\cdots$，

存在m，使得 $\eta(M_m)=\eta(M_{m+1})=\cdots$。

令 l 为 n, m 中的较大的一个，则有

$$M_l \cap N = M_{l+1} \cap N = \cdots, \quad \eta(M_l) = \eta(M_{l+1}) = \cdots.$$

此时有$M_l \subseteq M_{l+1} \subseteq \cdots$。考虑对任意一个 $t \geqslant l$，如果 $\alpha \in M_t$，由 $\eta(M_t) = \eta(M_l)$，则有 $\beta \in M_l$，使 $\alpha + N = \beta + N$。从而 $\alpha - \beta \in N$。又因为 $\beta \in M_l \subseteq M_t$，所以 $\alpha - \beta \in M_t$。这样，$\alpha - \beta \in M_t \cap N = M_l \cap N \subseteq M_l$，即有 $\alpha - \beta \in M_l$，$\alpha \in M_l$。由此可知$M_t \subseteq M_l$，即有$M_t = M_l$，故而得出：

$$M_l = M_{l+1} = \cdots.$$

亦即模M满足子模的升链条件。▮

命题4 设M为R—模，$M = M_1 + M_2$，$M_i (i = 1, 2)$是M的子模。那么，如果M_1，M_2都满足子模的升（降）链条件，则M也满足子模的升（降）链条件。

证 由第二同构定理，可得：

$$M/M_2 = (M_1 + M_2)\Big/M_2 \simeq M_1\Big/M_1 \cap M_2.$$

因为M_1满足升（降）链条件，从而它的商模$M_1\Big/M_1 \cap M_2$也满足升（降）链条件。于是，M/M_2也就满足升（降）链条件。这样，子模M_2与商模M/M_2同时满足升（降）链条件。因此，M满足升（降）链条件。▮

一个有恒等元素的环 R 自然可以看成 R 上的左（右）模。如果环R做为左（右）R—模是诺特（阿丁）模时，则称环 R 是左（右）诺特（阿丁）环。

命题5 设 R为有恒等元素的环。如果R是诺特（阿丁）环，那么R上的有限生成模是诺特（阿丁）模。

证 设M是R上的有限生成模，任取M的一组生成元素 α_1，α_2，…，α_n。则有

$$M = R\alpha_1 + R\alpha_2 + \cdots + R\alpha_n.$$

对这里的每一个循环模$R\alpha_i (i = 1, 2, \cdots, n)$，都有

$$R \sim R\alpha_i.$$

于是，如果环R做为模是诺特（阿丁）模，那么它的同态象 Ra_i $(i=1, 2, \cdots, n)$就也是诺特(阿丁)模。从而，根据命题4，即得模M是诺特（阿丁）模。▋

推论 设R为除环。那么R上的有限生成模M是诺特模，同时也是阿丁模。

事实上 对除环R来说，没有非平凡的左、右理想。因此，除环R当然是诺特环，同时也是阿丁环。因此，除环R上的有限生成模M既是诺特模又是阿丁模。▋

定理 R—模M是有限高的$\Longleftrightarrow M$同时满足子模的升链条件和降链条件。

证 如果M是有限高的，$h(M)=n$。考虑M的非平凡子模的真降的链：

$$N_1 \supset N_2 \supset \cdots \supset N_r.$$

从而相应的有一个子模塔

$$T: M \supset N_1 \supset N_2 \supset \cdots \supset N_r \supset \{0\},$$

其高 $h(T)=r+1$，于是，由§6 命题1，$r+1 \leqslant h(M)=n$。这就是说，模M的任一非平凡子模的真降（升）链中子模的个数必都小于M的高。由此便可肯定，模M不能有子模的无限真降(升)链，即，M满足子模的降链条件，也满足子模的升链条件。

其次，如果模M满足子模升链条件，也满足子模的降链条件。若$M=\{0\}$，当然是有限高的。若$M\neq\{0\}$，令$M=M_1$。于是，由升链条件，在M的真子模中必有极大的，任取其一，设为M_2。如果$M_2\neq\{0\}$。同理，在M_2的真子模中必有极大的，任取其一，设为M_3，但是，因为M满足子模的降链条件，这种做法不能无限的进行下去。于是，得到一个由有限个子模组成的真降链：

$$T: M=M_1 \supset M_2 \supset M_3 \supset \cdots \supset M_n \supset M_{n+1}=\{0\},$$

其中M_{i+1}是M_i的极大子模，$i=1, 2, \cdots, n$。这样，T恰是M的一个 Jordan—Hölder 塔，即M是有限高的，且$h(M)=n$。▋

可以认为，模M是有限高的这种性质是线性空间的有限维这种特殊性质的一种推广。我们在以上两节里，讨论了与有限高的模有关的一些基本性质。回过头来把这些性质和有限维线性空间的性质做些对比是有益的。

习　　题

1．证明：R—模M是诺特模$\Longleftrightarrow M$是有限生成模。

2．设R为有恒等元素，没有零因子的交换环。证明：环R看做R上的模是诺特模$\Longleftrightarrow R$是主理想环。

3．设R—模M，N都是诺特模，P为任一R—模，使得

$$0 \longrightarrow M \longrightarrow P \longrightarrow N \longrightarrow 0$$

是短正合列。证明：P的每一子模是诺特模。

4．把多项式环$\mathbf{Q}[x]$看成$\mathbf{Q}[x]$—模M。证明：M没有*Jordan—Hölder* 塔，但M的每一个真商模（即由非平凡子模确定的商模）都有 *Jordan—Hölder*塔。

5．令p为取定的素数，$\mathbf{C}_p=\{x\in\mathbf{C}\mid x^{p^k}=1$，对某一个$k=0，1，2，\cdots\}$。证明：把$\mathbf{C}_p$看成$\mathbf{Z}$—模时，它是阿丁模，但不是诺特模。

6．设σ是R—模M的一个自同态。证明：

（1）若M是诺特模，那么，σ是满同态$\Longleftrightarrow\sigma$是自同构。

（2）若M是阿丁模，那么，σ是单同态$\Longleftrightarrow\sigma$是自同构。

7．令V是域F上的线性空间。已知对V的任一线性变换σ，按

$$f(\lambda)\alpha=f(\sigma)(\alpha)$$

定义$F[\lambda]$与V到V的倍数乘法，使V做成一元多项式环$F[\lambda]$上的模。设V是在F上有可数基$\{\alpha_1，\alpha_2，\cdots\}$的无限维空间，证明：

（1）若线性变换 σ，使得

$$\sigma(\alpha_1)=0,\ \sigma(\alpha_{i+1})=\alpha_i,\ i=1,\ 2,\ \cdots.$$

那么$F[\lambda]$—模V是阿丁模。

（2）若取线性变换 τ，使得

$$\tau(\alpha_i)=\alpha_{i+1},\ i=1,\ 2,\ \cdots.$$

那么$F[\lambda]$—模V是诺特模。

§8 直　　和

本节讨论，从给定的 n 个R—模M_1，M_2，…，M_n做出一个R—模M的一般方法。同时，这也是把一个模 M 的结构的研究归结为去研究另外一些比较简单的模的结构的一种方法。

设M_1，M_2，…，M_n都是R—模。

首先做积集合$M=M_1\times M_2\times\cdots\times M_n$。即

$$M=\{(x_1,\ x_2,\ \cdots,\ x_n)\,|\,x_i\in M_i\},$$

此处，对M中的任二元素 $\alpha=(x_1,\ x_2,\ \cdots,\ x_n)$，$\beta=(y_1,\ y_2,\ \cdots,\ y_n)$，都有

$$\alpha=\beta\Longleftrightarrow x_1=y_1,\ x_2=y_2,\ \cdots,\ x_n=y_n.$$

其次，在M上规定加法如下：

$$(x_1,\ x_2,\ \cdots,\ x_n)+(y_1,\ y_2,\ \cdots,\ y_n)$$
$$=\ (x_1+y_1,\ x_2+y_2,\ \cdots,\ x_n+y_n)\ .$$

容易验证 $\{M;\ +\}$ 做成了一个加法群。其中元素 $\mathbf{0}=(0,\ 0,\ \cdots,\ 0)$ 是 $\{M;\ +\}$ 的零元素，并且

$$-(x_1,\ x_2,\ \cdots,\ x_n)=(-x_1,\ -x_2,\ \cdots,\ -x_n).$$

进而规定环R与加群M到M里的左倍数乘法如下：

$$k(x_1,\ x_2,\ \cdots,\ x_n)=(kx_1,\ kx_2,\ \cdots,\ kx_n).$$

同样不难指出，加法群M关于这样规定的左倍数乘法做成了环 R 上的模。我们把如此得到的R—模M叫做是M_1，M_2，…，M_n的（外）**直和**。记作 $M=M_1\oplus M_2\oplus\cdots\oplus M_n$，或$M=M_1\dot{+}M_2\dot{+}\cdots\dot{+}M_n$。

例1　数域F上的 n 元行空间 $F^{(n)}=\{(x_1,\ x_2,\ \cdots,\ x_n)\,|\,x_i\in F\}$ 是 n 个相同的模F的（外）直和，即有

$$F^{(n)}=F\oplus F\oplus\cdots\oplus F.$$

例2　令 $M_1=\mathbf{Z}_2=\{\overline{0},\ \overline{1}\}$，$M_2=\mathbf{Z}_3=\{\overline{0},\ \overline{1},\ \overline{2}\}$。于

是，有（外）直和$M=\mathbf{Z}_2\oplus\mathbf{Z}_3$，即

$$M=\{(\overline{0},\ \overline{0}),\ (\overline{0},\ \overline{1}),\ (\overline{0},\ \overline{2}),\ (\overline{1},\ \overline{0}),\ (\overline{1},\ \overline{1}),\ (\overline{1},\ \overline{2})\}.$$

例3 令$\mathbf{Z}$—模$M=\mathbf{Z}_6=\{\overline{0},\ \overline{1},\ \overline{2},\ \overline{3},\ \overline{4},\ \overline{5}\}$，取$M$的两个子模$M_1=\{\overline{0},\ \overline{3}\}$，$M_2=\{\overline{0},\ \overline{2},\ \overline{4}\}$。于是由$M_1$，$M_2$做成一个直和$M'=M_1\oplus M_2=\{(x,\ y)|x\in M_1,\ y\in M_2\}$。具体的写出$M'$的元素，即有

$$M'=\{(\overline{0},\ \overline{0}),\ (\overline{0},\ \overline{2}),\ (\overline{0},\ \overline{4}),\ (\overline{3},\ \overline{0}),\ (\overline{3},\ \overline{2}),\ (\overline{3},\ \overline{4})\}.$$

例4 令$\mathbf{Z}$—模$M_1=\mathbf{Z}$，$M_2=\mathbf{Z}_n=\{\overline{0},\ \overline{1},\ \overline{2},\cdots,\overline{n-1}\}$，做直和，则有

$$M=\mathbf{Z}\oplus\mathbf{Z}_n=\{(h,\ k)|h\in\mathbf{Z},\ k\in\mathbf{Z}_n\}.$$

设有（外）直和$M=M_1\oplus M_2\oplus\cdots\oplus M_n$。我们来分析每一个模$M_i$与直和$M$的关系。一般来说，不能认为$M_i\subseteq M$，这由上述各例可以明显地看出来。然而我们可以在直和M中找到一些子模$M'_i(i=1,\ 2,\ \cdots,\ n)$，它们与当初的$n$个模有着密切的联系，即依次的成同构。

命题1 设$M=M_1\oplus M_2\oplus\cdots\oplus M_n$。令

$$M'_i=\{(0,\ \cdots,\ 0,\ x_i,\ 0,\ \cdots,\ 0)|x_i\in M_i\},$$

$i=1,\ 2,\ \cdots,\ n$。

那么

（1）M'_i都是M的子模。

（2）在映射

$$\eta_i:(\cdots,\ x_i,\ \cdots)\longmapsto x_i$$

之下，M'_i与M_i是同构的，即$M'_i\overset{\eta_i}{\cong}M_i$。

（3）$M=M'_1+M'_2+\cdots+M'_n$。

(4) $M'_i \cap (M'_1+\cdots+M'_{i-1}+M'_{i+1}+\cdots+M'_n)=\{0\}$.

证 (1)与(2)都是很明显的。下面只对(3)和(4)说明如下。

$\forall \alpha=(x_1, x_2, \cdots, x_n)\in M$, 则有

$$\alpha=(x_1, 0, \cdots, 0)+(0, x_2, 0, \cdots, 0)+\cdots$$
$$+(0, \cdots, 0, x_n)\in M'_1+M'_2+\cdots+M'_n.$$

从而$M\subseteq M'_1+M'_2+\cdots+M'_n$, 所以(3)成立。

因为$M'_1+\cdots+M'_{i-1}+M'_{i+1}+\cdots+M'_n=\{(\cdots, x_{i-1}, 0, x_{i+1}, \cdots)|x_j\in M_j, j\neq i\}$. 于是, M'_i的元素$(\cdots, 0, x_i, 0, \cdots)$也是这个和里的元素当且仅当$x_i=0$. 从而说明(4)成立. ▮

定义 设M是R—模, M_1, M_2, $\cdots$, M_n是M的子模. 如果

(i) $M=M_1+M_2+\cdots+M_n$,

(ii) $M_j\cap(M_1+\cdots+M_{j-1}+M_{j+1}+\cdots+M_n)=\{0\}$, $j=1, 2, \cdots, n$.

则称模M是子模M_1, M_2, $\cdots$, M_n的(内)直和, 也说模M分解成子模M_1, M_2, $\cdots$, M_n的直和。

关于模M是子模M_1, M_2, $\cdots$, M_n的(内)直和的条件(i)与(ii)有时具体用起来不太方便. 下面给出用元素来表述的(内)直和条件。

命题2 模M是子模M_1, M_2, $\cdots$, M_n的(内)直和$\Longleftrightarrow$

(i)′ M中每一个元素α都可写成

$$\alpha=\alpha_1+\alpha_2+\cdots+\alpha_n, \quad \alpha_i\in M_i, \ i=1, 2, \cdots, n.$$

(ii)′ 上述的表示方法是唯一的, 即如果

$$\alpha=\alpha_1+\alpha_2+\cdots+\alpha_n=\beta_1+\beta_2+\cdots+\beta_n,$$
$$\alpha_i, \ \beta_i\in M_i,$$

必有$\alpha_i=\beta_i$ $(i=1, 2, \cdots, n)$

证 由(i)′$\Longrightarrow M=M_1+M_2+\cdots+M_n$, 如果有

$\alpha\in M_i\cap(M_1+\cdots+M_{i-1}+M_{i+1}+\cdots+M_n$, 则有

$\alpha=0+\cdots+0+\alpha_i+0+\cdots+0=\alpha_1+\cdots+\alpha_{i-1}+0+\alpha_{i+1}+0+\cdots+\alpha_n$，其中$\alpha_j\in M_j(j=1,\ 2,\ \cdots,n)$。于是，$\alpha_1=0,\ \alpha_2=0,\ \cdots,\ \alpha_i=0,\ \cdots,\ \alpha_n=0$，即$\alpha=0$，$M_i\cap(M_1+\cdots+M_{i-1}+M_{i+1}+\cdots+M_n)=\{0\}$。从而，$M$是$M_1$，$M_2$，…，$M_n$的（内）直和。

其次，如果M是子模M_1，M_2，…，M_n的（内）直和，$\Longrightarrow$ (i)′成立。若有 $\alpha=\alpha_1+\alpha_2+\cdots+\alpha_n=\beta_1+\beta_2+\cdots+\beta_n$，$\alpha_i$，$\beta_i\in M_i\Longrightarrow\alpha_1-\beta_1=(\beta_2-\alpha_2)+\cdots+(\beta_n-\alpha_n)\Longrightarrow\alpha_1-\beta_1=0$，即$\alpha_1=\beta_1$。同理可得$\alpha_2=\beta_2$，…，$\alpha_n=\beta_n$，即 (ii)′成立。▌

推论 模M是子模M_1，M_2，…，M_n的（内）直和$\Longleftrightarrow M$中每一个元素均能表成M_1，M_2，…，M_n中元素的和，而且零元素的表示法是唯一的，即

$$\alpha_1+\alpha_2+\cdots+\alpha_n=0\Longleftrightarrow\alpha_1=0,\ \alpha_2=0,\ \cdots,\ \alpha_n=0.$$

$\alpha_i\in M_i(i=1,\ 2,\ \cdots,\ n)$。▌

定理1 R—模M是子模M'_1，M'_2，…，M'_n的（内）直和$\Longleftrightarrow M$同构于模M_1，M_2，…，M_n的（外）直和，而有$M'_i\simeq M_i$ $(i=1,\ 2,\ \cdots,\ n)$。

证 充分性已如命题1所述。下面说明必要性成立。设模M是它的n个子模M'_1，M'_2，…，M'_n的（内）直和，且有n个R—模M_1，M_2，…，M_n，使得$M'_i\overset{\eta_i}{\simeq}M_i$ $(i=1,\ 2,\ \cdots,\ n)$。于是，由命题2，则有$\forall\alpha\in M$，都可唯一地写成

$$\alpha=\alpha'_1+\alpha'_2+\cdots+\alpha'_n,\quad \alpha'_i\in M'_i.\ i=1,\ 2,\ \cdots,\ n.$$

这样，令映射

$$\eta:\alpha'_1+\alpha'_2+\cdots+\alpha'_n\longmapsto(\eta_1(\alpha'_1),\ \eta_2(\alpha'_2),\ \cdots,\ \eta_n(\alpha'_n))=(\alpha_1,\ \alpha_2,\ \cdots,\ \alpha_n).$$

又由命题2，保证了η的合理性，进而容易知道η是M与（外）直和$M_1\oplus M_2\oplus\cdots\oplus M_n$的一个双射。且有

$$\eta[(\alpha'_1+\alpha'_2+\cdots+\alpha'_n)+(\beta'_1,\ \beta'_2,\ \cdots,\ \beta'_n)]$$

$$=\eta((\alpha_1'+\beta_1', \alpha_2'+\beta_2', \cdots, \alpha_n'+\beta_n'))$$
$$=(\eta_1(\alpha_1'+\beta_1'), \eta_2(\alpha_2'+\beta_2'), \cdots, \eta_n(\alpha_n'+\beta'))$$
$$=(\alpha_1+\beta_1, \alpha_2+\beta_2, \cdots, \alpha_n+\beta_n)$$
$$=(\alpha_1, \alpha_2, \cdots, \alpha_n)+(\beta_1, \beta_2, \cdots, \beta_n)$$
$$=\eta((\alpha_1', \alpha_2', \cdots, \alpha_n'))+\eta((\beta_1', \beta_2', \cdots, \beta_n')).$$
$$\eta(k(\alpha_1', \alpha_2', \cdots, \alpha_n'))=\eta((k\alpha_1', k\alpha_2', \cdots, k\alpha'))$$
$$=(\eta_1(k\alpha_1'), \eta_2(k\alpha_2'), \cdots, \eta_n(k\alpha_n'))$$
$$=(k\alpha_1, k\alpha_2, \cdots, k\alpha_n)=k(\alpha_1, \alpha_2, \cdots, \alpha_n)$$
$$=k\eta((\alpha_1', \alpha_2', \cdots, \alpha_n'))$$

即，η 是一个R—同构．所以$M\overset{\eta}{\simeq}M_1\oplus M_2\oplus\cdots\oplus M$ ▮

以上定理说明，模 M是模 M_1，M_2，…，M_n 的外直和或是它的子模M_1'，M_2'，…，M_n' 的内直和，就代数性质来说是没有本质区别的．因此，对于直和的说法我们不考虑外和内的差异．一律简称为直和，并且都用记号$M=M_1\oplus M_2\oplus\cdots\oplus M$ 表示模M是一个直和．

例5 $\mathbf{Z}$—模 $M=\mathbf{Z}_6=\{\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}, \overline{5}\}$．$M_1'=\{\overline{0}, \overline{3}\}$，$M_2'=\{\overline{0}, \overline{2}, \overline{4}\}$ 是$\mathbf{Z}_6$的两个子模，而且

$$M=M_1'+M_2'=M_1'\oplus M_2'.$$

如果取$M_1=\mathbf{Z}_2=\{\overline{0}, \overline{1}\}$，$M_2=\mathbf{Z}_3=\{\overline{0}, \overline{1}, \overline{2}\}$，则有直和

$$\overline{M}=M_1\oplus M_2=\{(\overline{0}, \overline{0}), (\overline{0}, \overline{1}), (\overline{0}, \overline{2}), (\overline{1}, \overline{0}), (\overline{1}, \overline{1}), (\overline{1}, \overline{2})\}.$$

于是，由$M_1'\overset{\eta_1}{\simeq}M_1$，$M_2'\overset{\eta_2}{\simeq}M_2$．从而有

$$M\overset{\eta}{\simeq}\overline{M}.$$

此处有

$$\eta_1: M_1'\longrightarrow M_1,\ \eta_1: \overline{0}\longmapsto\overline{0},\ \overline{3}\longmapsto\overline{1};$$

$\eta_2: M'_2 \longrightarrow M_2$, $\eta_2: \overline{0} \longmapsto \overline{0}$, $\overline{2} \longmapsto \overline{1}$, $\overline{4} \longmapsto \overline{2}$.

而映射 $\eta: M \longrightarrow \overline{M}$，使得

$$\eta: \overline{0} \longmapsto (\overline{0}, \overline{0}),\ \overline{1} \longmapsto (\overline{1}, \overline{2}),$$
$$\overline{2} \longmapsto (\overline{0}, \overline{1}),\ \overline{3} \longmapsto (\overline{1}, \overline{0}),$$
$$\overline{4} \longmapsto (\overline{0}, \overline{2}),\ \overline{5} \longmapsto (\overline{1}, \overline{1}).$$

从叙述过程中，明显可知，$M = M'_1 \oplus M'_2$是内直和，而$\overline{M} = M_1 \oplus M_2$是外直和。

命题3 如果$M = M_1 \oplus M_2 \oplus \cdots \oplus M_n$. 那么对任意的$1 < n_1 < n_2 < \cdots < n_s = n$，都有

$$N_1 = M_1 + \cdots + M_{n_1} = M_1 \oplus \cdots \oplus M_{n_1}$$
$$N_2 = M_{n_1+1} + \cdots + M_{n_2} = M_{n_1+1} \oplus \cdots \oplus M_{n_2},$$
$$\cdots \qquad \cdots \qquad \cdots$$
$$N_s = M_{n_{s-1}+1} + \cdots + M_{n_s} = M_{n_{s-1}+1} \oplus \cdots \oplus M_{n_s}.$$

以及

$$M = N_1 \oplus N_2 \oplus \cdots \oplus N_{n_s}.$$

反之，如果$M = N_1 \oplus N_2 \oplus \cdots \oplus N_S$，而且

$N_1 = M_1 \oplus \cdots \oplus M_{n_1}$, $N_2 = M_{n_1+1} \oplus \cdots \oplus M_{n_2}$, $\cdots$,

$N_s = M_{n_{s-1}+1} \oplus \cdots \oplus M_{n_S}$，那么 $M = M_1 \oplus \cdots \oplus M_{n_1} \oplus M_{n_1+1} \oplus \cdots \oplus M_{n_2} \oplus \cdots \oplus M_{n_{s-1}+1} \oplus \cdots \oplus M_{n_s}$.

命题4 如果$M = M_1 \oplus M_2$，那么$M_1 \simeq M/M_2$，$M_2 \simeq M/M_1$.

以上两个命题的证明都做为习题，留给读者去做。

本节最后讨论直和分解式$M = M_1 \oplus M_2 \oplus \cdots \oplus M_n$与模$M$的自同态之间的重要联系。从而给出用$M$的自同态来刻划模$M$分解成为子模的直和的可能性。

设$M = M_1 \oplus M_2 \oplus \cdots \oplus M$ ，于是对任一$a \in M$，则有

$$\alpha = \alpha_1 + \alpha_2 + \cdots + \alpha_n,\ \alpha_i \in M_i,$$

而且这种表示法是唯一的，考虑以下一组映射：

$$\begin{aligned} &\varepsilon_1 : \alpha = \alpha_1 + \alpha_2 + \cdots + \alpha_n \longmapsto \alpha_1, \\ &\varepsilon_2 : \alpha = \alpha_1 + \alpha_2 + \cdots + \alpha_n \longmapsto \alpha_2, \\ &\cdots \qquad \cdots \qquad \cdots \\ &\varepsilon_n : \alpha = \alpha_1 + \alpha_2 + \cdots + \alpha_n \longmapsto \alpha_n \end{aligned} \tag{1}$$

容易知道，$\varepsilon_i (i = 1, 2, \cdots, n)$ 都是模M的自同态，并且

$\varepsilon_i(M) = M_i$，$\varepsilon_i|_{M_i} = 1_{M_i}$，$\varepsilon_i|_{M_j} = 0_{M_j}$，$(i = 1, 2, \cdots, n;\ j \neq i)$ 于是可得：

$$\varepsilon_i^2(\alpha) = \varepsilon_i(\varepsilon_i(\alpha)) = \varepsilon_i(\alpha_i) = \alpha_i = \varepsilon_i(\alpha) \Longrightarrow \varepsilon_i^2 = \varepsilon_i,$$

$$\varepsilon_i\varepsilon_j(\alpha) = \varepsilon_i(\varepsilon_j(\alpha)) = \varepsilon_i(\alpha_j) = 0, \Longrightarrow \varepsilon_i\varepsilon_j = 0,\ (i \neq j),$$

同理，$\varepsilon_j\varepsilon_i = 0$

$$\begin{aligned} (\varepsilon_1 + \varepsilon_2 + \cdots + \varepsilon_n)(\alpha) &= \varepsilon_1(\alpha) + \varepsilon_2(\alpha) + \cdots + \varepsilon_n(\alpha) \\ &= \alpha_1 + \alpha_2 + \cdots + \alpha_n = \alpha. \end{aligned}$$

$\Longrightarrow \varepsilon_1 + \varepsilon_2 + \cdots + \varepsilon_n = 1_M$。

概括起来，即有：若模M分解成子模 M_1，M_2，$\cdots$，M_n 的直和：$M = M_1 \oplus M_2 \oplus \cdots \oplus M_n$，那么由（1）有模$M$的$n$个自同态 ε_1，ε_2，$\cdots$，ε_n 具有以下性质：

（i） $\varepsilon_i^2 = \varepsilon_i$，$i = 1, 2, \cdots, n$.

（ii） $\varepsilon_i\varepsilon_j = 0 = \varepsilon_j\varepsilon_i$，$i \neq j$.

（iii） $\varepsilon_1 + \varepsilon_2 + \cdots + \varepsilon_n = 1_M$.

我们把这样得到的模 M的n个自同态 ε_1，ε_2，$\cdots$，ε_n 叫做与直和$M = M_1 \oplus M_2 \oplus \cdots \oplus M_n$相伴的一组自同态.

现在反过来看，如果模M有一组自同态 ε_1，ε_2，$\cdots$，ε_n 具有以上三条性质，那么，令

$$\varepsilon_1(M) = M_1,\ \varepsilon_2(M) = M_2,\ \cdots,\ \varepsilon_n(M) = M_n$$

则得M的 n 个子模M_1，M_2，$\cdots$，M_n. 于是，由（iii）成立，$\forall \alpha \in M$，则有

$$a=(\varepsilon_1+\varepsilon_2+\cdots+\varepsilon_n)(a)=\varepsilon_1(a)+\varepsilon_2(a)+\cdots+\varepsilon_n(a)$$

可知$M=M_1+M_2+\cdots+M_n$。

进而，若 $a_1+a_2+\cdots+a_n=0$，$a_i\in M_i$，则有

$$0=\varepsilon_i(0)=\varepsilon_i(a_1+a_2+\cdots+a_n)$$
$$=\varepsilon_i(a_1)+\varepsilon_i(a_2)+\cdots+\varepsilon_i(a_n)=a_i$$

从而，模M是子模M_1，M_2，…，M_n的直和：$M=M_1\oplus M_2\oplus\cdots\oplus M_n$。

我们把满足条件（i）、（ii）、（iii）的模M的n个自同态ε_1，ε_2，…，ε_n按以上方法确定的模M的直和分解式：$M=M_1\oplus M_2\oplus\cdots\oplus M_n$叫做与自同态$\varepsilon_1$，$\varepsilon_2$，…，$\varepsilon_n$相伴的直和分解式。

不难知道，如果与直和分解式$M=M_1\oplus M_2\oplus\cdots\oplus M_n$相伴的自同态是$\varepsilon_1$，$\varepsilon_2$，…，$\varepsilon_n$，那么与这组自同态相伴的直和分解式就正好是$M=M_1\oplus M_2\oplus\cdots\oplus M_n$。反之亦然。

如果我们把满足条件（i），（ii）和（iii）的模M的n个自同态ε_1，ε_2，…，ε_n叫做M的一组完全的正交射影，那么我们已经证明了如下的

定理2 R—模M能够分解成n个子模的直和$\Longleftrightarrow$模M有由n个自同态组成的一组完全的正交射影。∎

习　题

1．举例说明：R—模M的子模M_1，M_2，…，M_n，如果满足条件：

（i）　$M=M_1+M_2+\cdots+M_n$，

（ii）　$\forall i\neq j$，$M_i\cap M_j=\{0\}$，

M未必是子模M_1，M_2，…，M_n的直和。

如果把条件（ii）加强为

$$(\text{ii})' \quad M_i \cap \left(\bigcup_{j \neq i} M_j \right) = \{0\},$$

结论又如何？

2. 设 R—模 $M = M_1 + M_2 + \cdots + M_n$，子模 $M_i (i = 1, 2, \cdots, n)$ 满足以下条件：

$$M_1 \cap M_2 = \{0\},$$
$$(M_1 + M_2) \cap M_3 = \{0\},$$
$$\vdots$$
$$(M_1 + M_2 + \cdots + M_{n-1}) \cap M_n = \{0\},$$

证明：$M = M_1 \oplus M_2 \oplus \cdots \oplus M_n$。

3. 把$\mathbf{Z}_n$看成$\mathbf{Z}$—模，证明：若 $n = p^l$，p为素数，$l > 0$。那么$\mathbf{Z}_n$不能分解成两个非零子模的直和，把整数加法群 $\mathbf{Z}$看成$\mathbf{Z}$—模时，这个结论成立吗？对另外的正整数 n（$\neq p^l$），这个结论对$\mathbf{Z}_n$成立吗？

4. 设R—模$M = M_1 \oplus M_2 \oplus \cdots \oplus M$ ，N_i是M_i的子模（$i = 1, 2, \cdots, n$）证明：

（1） $N = \sum\limits_{i=1} N_i = N_1 \oplus N_2 \oplus \cdots \oplus N_n$，

（2） $M/N \simeq M_1/N_1 \oplus M_2/N_2 \oplus \cdots \oplus M_n/N$ 。

5. 设 σ 是R—模M的自同态，证明：若 $M = Im\sigma \oplus ker\sigma$则 $Im\sigma = Im\sigma^2$。

6. 设 $\sigma: M \longrightarrow N$，$\tau: N \longrightarrow M$都是 R— 同 态，使 $\tau\sigma = 1_M$。证明：$N = Im\sigma \oplus ker\tau$。

7. 证明命题3。

8. 证明命题4。

9. 设σ 是R—模 M的自同态。证明：如果 $\sigma^2 = \sigma$，则存在子模P，N使$M = P \oplus N$，并且$\sigma|_P = 1_P$，$\sigma|_N = 0_N$（通常称这样的自同态 σ 是模M的平行于子模N，在子模P上的射影）。

§9 不可分解模 Krull—Schmidt定理

本节讨论一般R—模的直和分解问题. 对于特殊的模—域F上的线性空间V，有大家都很熟悉的重要性质：V是有限维的$\Longleftrightarrow$ V能分解成有限个一维子空间(子模)的直和. 换个说法是：V是n维线性空间$\Longleftrightarrow$$V$能分解成$n$个一维子空间的直和，而且显然的，其中每一个一维子空间都不能再分解为非平凡的子空间的直和. 无疑的，一个线性空间有否这样的直和分解式，对于它的结构来说是一个十分重要的特征性质. 在这一节里，我们将把线性空间是有限维的特征性质的这种形式的描述推广到一般的R—模上去，讨论R—模M具有类似的直和分解式的条件和唯一性问题.

定义 设M为R—模，$M\neq\{0\}$. 如果M能够表成两个非平凡子模的直和，即$M=M_1\oplus M_2$，其中$M_i\neq M(i=1, 2)$，则称模M是可分解的. 否则，就说M是不可分解的.

例1 任一单模M必是不可分解的. 因为它没有非平凡子模. $\mathbf{Z}$与$\mathbf{Z}_4$虽然都不是单模，但二者都是不可分解的. 由此可见，M是单模$\Longrightarrow$$M$不可分解，反之则未必.

例2 自然的，$M=\mathbf{Z}\oplus\mathbf{Z}_4$做为$\mathbf{Z}$上的模是可分解的. 再有，令环

$$R=\left\{\begin{pmatrix}a_{11} & a_{12} & a_{13}\\ a_{21} & a_{22} & a_{23}\\ a_{31} & a_{32} & a_{33}\end{pmatrix}\middle|\ a_{ij}\in Q\right\}.$$

把R的加法群$M=\{R;\ +\}$看成R—模. 则有

$$M_1=\left\{\begin{pmatrix}a_{11} & 0 & 0\\ a_{21} & 0 & 0\\ a_{31} & 0 & 0\end{pmatrix}\middle|\ a_{11},\ a_{21},\ a_{31}\in\mathbf{Q}\right\},$$

$$M_2 = \left\{ \begin{pmatrix} 0 & a_{12} & 0 \\ 0 & a_{22} & 0 \\ 0 & a_{32} & 0 \end{pmatrix} \middle| a_{12}, a_{22}, a_{32} \in \mathbf{Q} \right\},$$

$$M_3 = \left\{ \begin{pmatrix} 0 & 0 & a_{13} \\ 0 & 0 & a_{23} \\ 0 & 0 & a_{33} \end{pmatrix} \middle| a_{13}, a_{23}, a_{33} \in \mathbf{Q} \right\},$$

是M的三个非平凡子模，而且使

$$M = M_1 \oplus M_2 \oplus M_3$$

所以，M是可分解的。其中每一个子模 M_i 都不能分解成两个非平凡子模的直和，即M_i都是不可分解的模。

例3 设R—模$M \neq \{0\}$。那么，M是不可分解的$\Longleftrightarrow$自同态环$End_R M$中除了0，1之外，没有非平凡的射影σ（即$\sigma^2 = \sigma$）。

证 如果模M是可分解的，即有非平凡子模M_1，M_2，使$M = M_1 \oplus M_2$，于是，由§8定理2，有与这个直和分解式相伴的一组完全的正交射影ε_1，ε_2。因为M_1，M_2是非平凡的子模，从而 ε_1，ε_2 也是非平凡的射影。

反之，如果 $End_R M$中存在射影 σ，且$\sigma \neq 0$，$\sigma \neq 1$。那么令 $\varepsilon_1 = \sigma$，$\varepsilon_2 = 1 - \sigma$。则有

$$\varepsilon_1^2 = \varepsilon_1, \quad \varepsilon_2^2 = (1-\sigma)^2 = (1-\sigma)(1-\sigma) = 1 - 2\sigma + \sigma^2$$

$$= 1 - \sigma = \varepsilon_2.$$

$$\varepsilon_1\varepsilon_2 = \sigma(1-\sigma) = \sigma - \sigma^2 = 0, \quad \varepsilon_2\varepsilon_1 = (1-\sigma)\sigma = \sigma - \sigma^2 = 0,$$

$$\varepsilon_1 + \varepsilon_2 = \sigma + (1-\sigma) = 1.$$

这就说明，ε_1，ε_2 是 M 的一组完全的正交射影。于是有与其相伴的模 M 的直和分解式：$M = M_1 \oplus M_2$。其中$M_1 = \varepsilon_1(M)$，$M_2 = \varepsilon_2(M)$。由于 $\varepsilon_i \neq 0$，1，可知$M_i \neq \{0\}$($M_i \neq M$)，$i = 1$，2。从而，模M是可分解的。

定理1 若R—模M满足子模的两个链条件，那么M包含有限个不可分解的子模$M_1, M_2, \cdots, M_n$，使$M = M_1 \oplus M_2 \oplus \cdots \oplus M_n$。

证 由模M满足子模的两个链条件，可知M是有限高的。这

样，我们对模M的高 $h(M)$ 用数学归纳法证明定理 1 成立。

首先，当 $h(M)=1$ 时，则M是单模，自然的，M 是不可分解的，于是$M=M$，即合所求。

其次，归纳假设对 $h(M)<m$ 的情形，定理 1 成立。进而看$h(M)=m$的情形。

若M本身是不可分解的，则定理 1 的结论自然成立。若 M是可分解的。令 $M=M_1\oplus M_2$，其中$M_i\neq M(i=1, 2)$。于是$h(M_i)<h(M)$。由归纳法假设，则有

$$M_1=M_{11}\oplus M_{12}\oplus\cdots\oplus M_{1n_1},$$

$$M_2=M_{21}\oplus M_{22}\oplus\cdots\oplus M_{2n_2},$$

其中M_{ij}均为不可分解的。

这样，$M=M_{11}\oplus M_{12}\oplus\cdots\oplus M_{1n_1}\oplus M_{21}\oplus M_{22}\oplus\cdots\oplus M_{2n_2}$

即合所求。∎

定理 1 给出了，R—模 M 可以表成有限个不可分解的子模的直和的充分条件。在这样的前提下，为了解决分解的唯一性问题，我们需要以下两个预备性的事实。这两个结果本身也有独立的重要意义。

命题1 设R—模M满足子模的两个链条件。σ 是M的一个自同态。那么

（1）如果 σ 是单的，则 σ 是自同构。

（2）如果 σ 是满的，则 σ 是自同构。

证 先证（1）成立。设 σ 是单的，去证 σ 也是满的就行了，即 $M=\sigma(M)$。用反证法，如果 σ 不是满的，则有子模的降链：

$$M\supseteq\sigma(M)\supseteq\sigma^2(M)\supseteq\cdots\supseteq\sigma^{r-1}(M)\supseteq\sigma^r(M)\supseteq\sigma^{r+1}(M)\supseteq\cdots.$$

因为M满足降链条件，则有 r 使得

$$M\supset\sigma(M)\supset\cdots\supset\sigma^{r-1}(M)\supset\sigma^r(M)=\sigma^{r+1}(M)=\cdots.$$

其中$r>0$，因此，$\forall\beta\in\sigma^{r-1}(M)\Longrightarrow\sigma(\beta)\in\sigma^r(M)=\sigma^{r+1}(M)$．从而，有 $\alpha\in M$，使 $\sigma(\beta)=\sigma^{r+1}(\alpha)$．即$\sigma(\beta)=\sigma(\sigma^r(\alpha))$．由于$\sigma$是单的，则得 $\beta=\sigma^r(\alpha)$，$\beta\in\sigma^r(M)$，$\sigma^{r-1}(M)\subseteq\sigma^r(M)$．故而 $\sigma^{r-1}(M)=\sigma^r(M)$，这个矛盾的结果说明 $M\supset\sigma(M)$ 是不可能的。所以必有$M=\sigma(M)$，即σ是满的，亦即σ是M的自同构．

其次证（2）成立，设σ是满的，即 $\sigma(M)=M$．去证σ也是单的就行了，即 $ker\,\sigma=\{0\}$．用反证法，如果σ不是单的，则有子模的升链：

$$\{0\}\subseteq ker\sigma\subseteq ker\sigma^2\subseteq\cdots\subseteq ker\sigma^{s-1}\subseteq ker\sigma^s\subseteq ker\sigma^{s+1}\subseteq\cdots.$$

因为M满足子模的升链条件，则有s使得

$$\{0\}\subset ker\sigma\subset ker\sigma^2\subset\cdots\subset ker\sigma^{s-1}\subset ker\sigma^s=ker\sigma^{s+1}=\cdots.$$

其中 $s>0$．因此，$\forall\beta\in ker\sigma^s$，由于$\sigma$是满的，则有$\alpha\in M$．使 $\beta=\sigma(\alpha)$．于是

$$\sigma^{s+1}(\alpha)=\sigma^s(\sigma(\alpha))=\sigma^s(\beta)=0\Longrightarrow\alpha\in ker\sigma^{s+1}=ker\sigma^s$$

$\Longrightarrow\sigma^s(\alpha)=0$，$\sigma^{s-1}(\sigma(\alpha))=\sigma^{s-1}(\beta)=0$，即$\beta\in ker\sigma^{s-1}$，$ker\sigma^s\subseteq ker\sigma^{s-1}$，从而$ker\sigma^{s-1}=ker\sigma^s$．这个矛盾的结果说明，$\{0\}\subset ker\sigma$是不可能的，所以$ker\sigma=\{0\}$，即$\sigma$也是单的，亦即$\sigma$是$M$的自同构．∎

命题2 （*Fitting*引理）设R—模M满足子模的两个链条件．那么对M的任意一个自同态σ，都有直和分解式：

$$M=N\oplus H$$

使得σ在子模N上的限制$\sigma|_N$是N的幂零自同态，在子模H上的限制$\sigma|_H$是H的一个自同构．

证 考虑由σ所确定的两个子模链：

$$\{0\}\subseteq ker\sigma\subseteq ker\sigma^2\subseteq\cdots\subseteq ker\sigma^s\subseteq\cdots,$$

$$M\supseteq\sigma(M)\supseteq\sigma^2(M)\supseteq\cdots\supseteq\sigma^r(M)\supseteq\cdots.$$

因为M满足子模的两个链条件，那么必有s和r，使得

$$ker\sigma^s=ker\sigma^{s+1}=\cdots,$$

$$\sigma^r(M)=\sigma^{r+1}(M)=\cdots.$$

令$N=ker\sigma^t$，$H=\sigma^t(M)$，$t=max(s, r)$。

于是，$\forall\alpha\in M$，$\sigma^t(\alpha)\in\sigma^t(M)=\sigma^{2t}(M)$，则有$\beta\in M$，使$\sigma^t(\alpha)=\sigma^{2t}(\beta)$。即$\sigma^t(\alpha-\sigma^t(\beta))=0$。这样，便可把元素$\alpha$表示成

$$\alpha=(\alpha-\sigma^t(\beta))+\sigma^t(\beta),$$

其中$\sigma^t(\alpha-\sigma^t(\beta))=0$，即$\alpha-\sigma^t(\beta)\in ker\sigma^t=N$，而且$\sigma^t(\beta)\in\sigma^t(M)=H$。由此可知，$M=N+H$。为了肯定这个和还是直和，令$\alpha\in N\cap H$，那么$\alpha\in H\Longrightarrow\alpha=\sigma^t(\beta)$，$\beta\in M$。由$\alpha\in N$，则有$\sigma^t(\alpha)=0\Longrightarrow\sigma^{2t}(\beta)=\sigma^t(\sigma^t(\beta))=\sigma^t(\alpha)=0$，即$\beta\in N$即有$\sigma^t(\beta)=0$，亦即$\alpha=0$。所以有直和分解式$M=N\oplus H$。

σ在子模N上的限制显然是幂零自同态。而由$\sigma^t(M)=\sigma^{t+1}(M)$，即$H=\sigma(H)$，这说明，$\sigma$在子模$H$上的限制$\sigma|_H$是$H$本身的一个自同态，并且是满同态。于是，由命题1，即知$\sigma|_H$是H的一个自同构。∎

推论1 设R—模M满足子模的两个链条件。如果M是不可分解的，那么M的自同态σ或者是幂零的或者是自同构。

证 由命题2，可令$M=N\oplus H$，使σ在N上看是幂零自同态，而在H上看是一个自同构。如果M是不可分解的，那么或者$M=N$，或者$M=H$。当$M=N$时，σ就是M的幂零自同态，当$M=H$时，σ就是M的一个自同构。∎

推论2 设R—模M满足子模的两个链条件。如果M是不可分解的，那么M的任意两个幂零自同态σ_1，σ_2之和$\sigma_1+\sigma_2$也是幂零自同态。一般地，任意n个幂零自同态之和也是幂零自同态。

证 用反证法，如果幂零自同态σ_1，σ_2之和$\sigma=\sigma_1+\sigma_2$不是幂零的，则由推论1，$\sigma_1+\sigma_2$是M的一个自同构。这样就有自同构σ^{-1}。于是，$\sigma^{-1}\sigma=1_M$，即$\sigma^{-1}\sigma_1+\sigma^{-1}\sigma_2=1$。令$\sigma^{-1}\sigma_1=\tau_1$，$\sigma^{-1}\sigma_2=\tau_2$，不难知道，$\tau_1$，$\tau_2$都不能是自同构。从而都是幂零的。而且，由

$$\tau_1=\tau_1(\tau_1+\tau_2)=\tau_1^2+\tau_1\tau_2,\quad \tau_1=(\tau_1+\tau_2)\tau_1=\tau_1^2+\tau_2\tau_1$$

$$\Longrightarrow\tau_1\tau_2=\tau_2\tau_1.$$

这样，对任一正整数m，有

$$\left(\tau_1+\tau_2\right)^m=\tau_1^m+\binom{m}{1}\tau_1^{m-1}\tau_2+\binom{m}{2}\tau_1^{m-2}\tau_2^2+\cdots+$$

$$\binom{m}{m-1}\tau_1\tau_2^{m-1}+\tau_2^m.$$

由τ_1，τ_2都是幂零的，则有$\tau_1^s=0$，$\tau_2^r=0$，于是当取$m=s+r-1$时，则得 $(\tau_1+\tau_2)^m=0$ 。但 $\tau_1+\tau_2=1$，从而，这个矛盾的结果说明，$\sigma_1+\sigma_2$不可能不是幂零的，即$\sigma_1+\sigma_2$ 必是幂零的。而对一般的情形，对σ的个数用归纳法，即可得到证明。▮

通常把 *Fitting* 引理中的直和分解式叫做模M关于自同态σ的 *Fitting* **分解**。可以证明，对于给定的一个自同态σ，*Fitting* 分解是唯一的（习题5）。

有了以上的准备，现在我们就来证明本节的主要定理，即通常所说的 *Krull—Schmidt* 定理。

定理2 （*Krull—Schmidt* 定理）设R—模M满足子模的两个链条件。如果模M有两个直和分解式：

$$M=N_1\oplus N_2\oplus\cdots\oplus N_s,$$

$$M=H_1\oplus H_2\oplus\cdots\oplus H_t,$$

其中N_i，H_j $(i=1, 2, \cdots, s;\ j=1, 2, \cdots, t)$ 都是不可分解的；那么

（1）$s=t$

（2）适当编排H_1，H_2，$\cdots$，H_t 的顺序后，则有

$$N_1\simeq H_1,\ N_2\simeq H_2,\ \cdots,\ N_s\simeq H_s,$$

并且对任意的 $k=1, 2, \cdots, s$，都有

$$M=H_1\oplus H_2\oplus\cdots\oplus H_k\oplus N_{k+1}\oplus\cdots\oplus N_s.$$

证 不妨认为 $s\leqslant t$。于是，令

σ_1，σ_2，$\cdots$，σ_s 是与$M=N_1\oplus N_2\oplus\cdots\oplus N_s$ 相伴的一组完全

的正交射影。$\tau_1, \tau_2, \cdots, \tau_t$ 是与$M=H_1\oplus H_2\oplus\cdots\oplus H_t$相伴的一组完全的正交射影。

我们的证明想法是：从分解式$M=N_1\oplus N_2\oplus\cdots\oplus N_s$中的子模$N_1$开始，在分解式$M=H_1\oplus H_2\oplus\cdots\oplus H_t$中找到一个与$N_1$同构的子模，比如说是$H_1$，并且用这个$H_1$替换$N_1$之后还是模$M$的一个直和分解式：$M=H_1\oplus N_2\oplus\cdots\oplus N_s$。接着，再从这个分解式中的$N_2$出发，去在分解式$M=H_1\oplus H_2\oplus\cdots\oplus H_t$中找一个与$N_2$同构的子模，比如说是$H_2$，并且，…。

为了实现这样的证明想法，首先考察$\sigma_1\tau_1, \sigma_1\tau_2, \cdots, \sigma_1\tau_t$。明显可知，这$t$个乘积的每一个在子模$M_1$上的限制$\sigma_1\tau_i|_{N_1}$（即只看$\sigma_1\tau_i$在$N_1$上的作用）都是$N_1$的自同态。因为$N_1$也满足子模的两个链条件，而且$N_1$是不可分解的。由Fitting引理的推论1，每一$\sigma_1\tau_i|_{N_1}$或是幂零的或是自同构。又因为

$$\sigma_1=\sigma_1\tau_1+\sigma_1\tau_2+\cdots+\sigma_1\tau_t,$$

$$\sigma_1|_{N_1}=1_{N_1}=(\sigma_1\tau_1+\sigma_1\tau_2+\cdots+\sigma_1\tau_t)|_{N_1}.$$

由Fitting引理的推论2，不可能每一个$\sigma_1\tau_i|_{N_1}$都是幂零的。从而只少有一个$\sigma_1\tau_i|_{N_1}$是N_1的自同构。不失一般性，不妨认为$\sigma_1\tau_1|_{N_1}$是N_1的自同构。令$\tau_1(N_1)=\overline{H}_1$，则$\overline{H}_1\subseteq H_1$。于是有$N_1\overset{\tau_1}{\sim}\overline{H}_1$，$\overline{H}_1\overset{\sigma_1}{\sim}N_1$。我们指出这两个同态其实都是同构。事实上，若$\alpha\in N_1$，有$\tau_1(\alpha)=0\Longrightarrow\sigma_1(\tau_1(\alpha))=\sigma_1\tau_1(\alpha)=0$。但$\sigma_1\tau_1$在$N_1$看是自同构。从而$\alpha=0$。这就说明$\tau_1$在$N_1$中的核为$\{0\}$。即有$N_1\overset{\tau_1}{\simeq}\overline{H}$，类似地，也有$\overline{H}_1\overset{\sigma_1}{\simeq}N_1$。

至此，我们迫切地需要指明：$\overline{H}_1=H_1$。为此，令$K_1=\{\alpha\in H_1|\sigma_1(\alpha)=0\}$，它是$H_1$的一个子模。于是，$\forall\alpha\in H_1$，$\sigma_1(\alpha)\in N_1$。由$\sigma_1\tau_1$是$N_1$的自同构，则有$\beta\in N_1$，使$\sigma_1(\alpha)=\sigma_1\tau_1(\beta)$，即$\sigma_1(\alpha-\tau_1(\beta))=0$。这样，元素$\alpha$可以写成

$$\alpha=[\alpha-\tau_1(\beta)]+\tau_1(\beta),$$

其中 $\alpha-\tau_1(\beta)\in K_1$，$\tau_1(\beta)\in\overline{H_1}$．这说明$H_1$是子模$K_1$与$\overline{H_1}$的和，即$H_1=K_1+\overline{H_1}$．并且，如果$\alpha\in K_1\cap\overline{H_1}$，由于$\sigma_1$是$\overline{H_1}$与$N_1$的同构映射，即知$\overline{H_1}$中只有零元素，在$\sigma_1$之下的象是0，从而可知$\alpha=0$，这样就有$H_1=K_1\oplus\overline{H_1}$．然而，$H_1$是不可分解的，而且$N_1\overset{\tau_1}{\simeq}\overline{H_1}$，可知$\overline{H_1}\neq\{0\}$．从而必有$K_1=\{0\}$，即$H_1=\overline{H_1}$．亦即$N_1\overset{\tau_1}{\simeq}H_1$，$H_1\overset{\sigma_1}{\simeq}N_1$．

这样，我们找到了与N_1同构的子模H_1．下面指出，可以用H_1替换N_1，使$M=H_1\oplus N_2\oplus\cdots\oplus N_s$．为此令$M'=H_1+N_2+\cdots+N_s$．因为$\sigma_1(N_2+\cdots+N_s)=\{0\}$，而$H_1\overset{\sigma_1}{\simeq}N_1$．可知，$H_1\cap(N_2+\cdots+N_s)=\{0\}$．从而有

$$M'=H_1\oplus(N_2+\cdots+N_s)=H_1\oplus N_2\oplus\cdots\oplus N_s.$$

于是，令

$$\eta:\alpha_1+\alpha_2+\cdots+\alpha_s\longmapsto\tau_1(\alpha_1)+\alpha_2+\cdots+\alpha_s.$$

其中 $\alpha_i\in N_i$，$i=1, 2, \cdots, s$.

那么，η 是$M=N_1\oplus N_2\oplus\cdots\oplus N_s$到$M'$的一个双射．而且

$$\begin{aligned}
&\eta((\alpha_1+\alpha_2+\cdots+\alpha_s)+(\beta_1+\beta_2+\cdots+\beta_s))\\
&=\eta((\alpha_1+\beta_1)+(\alpha_2+\beta_2)+\cdots+(\alpha_s+\beta_s))\\
&=\tau_1(\alpha_1+\beta_1)+(\alpha_2+\beta_2)+\cdots+(\alpha_s+\beta_s)\\
&=(\tau_1(\alpha_1)+\tau_1(\beta_1))+(\alpha_2+\beta_2)+\cdots+(\alpha_s+\beta_s)\\
&=(\tau_1(\alpha_1)+\alpha_2+\cdots+\alpha_s)+(\tau_1(\beta_1)+\beta_2+\cdots+\beta_s)\\
&=\eta(\alpha_1+\alpha_2+\cdots+\alpha_s)+\eta(\beta_1+\beta_2+\cdots+\beta_s)
\end{aligned}$$

$$\begin{aligned}
&\eta(k(\alpha_1+\alpha_2+\cdots+\alpha_s))=\eta(k\alpha_1+k\alpha_2+\cdots+k\alpha_s)\\
&=\tau_1(k\alpha_1)+k\alpha_2+\cdots+k\alpha_s\\
&=k\tau_1(\alpha_1)+k\alpha_2+\cdots+k\alpha_s\\
&=k(\tau_1(\alpha_1)+\alpha_2+\cdots+\alpha_s)
\end{aligned}$$

$$= k\eta(\alpha_1 + \alpha_2 + \cdots + \alpha_s)$$

其中 α_i, $\beta_i \in N_i$, $k \in R$, $i = 1, 2, \cdots, s$.

这就说明，$M \overset{\eta}{\simeq} M'$. 因为$M' \subseteq M$，即 η 是模 M 的一个自同态，而且 η 是单的，这样，根据命题1，可知 η 是M的自同构，从而 η也是满的. 故有，$M' = M$. 即$M = H_1 \oplus N_2 \oplus \cdots \oplus N_s$.

接着，考察M的两个分解式：

$$M = H_1 \oplus N_2 \oplus N_3 \oplus \cdots \oplus N_s$$

$$M = H_1 \oplus H_2 \oplus H_3 \oplus \cdots \oplus H_t.$$

对$M = H_1 \oplus N_2 \oplus N_3 \oplus \cdots \oplus N_s$的子模$N_2$，去在$M = H_1 \oplus H_2 \oplus \cdots \oplus H_t$中找一个与$N_2$同构的子模. 为此，令 ρ_1, ρ_2, ρ_3, $\cdots$, ρ_s是与直和分解式

$$M = H_1 \oplus N_2 \oplus N_3 \oplus \cdots \oplus N_s$$

相伴的一组完全的正交射影；τ_1, τ_2, τ_3, $\cdots$, τ_t还是与

$$M = H_1 \oplus H_2 \oplus H_3 \oplus \cdots \oplus H_t$$

相伴的一组完全的正交射影. 这样，$\rho_2\tau_1$, $\rho_2\tau_2$, $\rho_2\tau_3$, $\cdots$, $\rho_2\tau_t$的每一个在子模N_2上的限制 $\rho_2\tau_i|_{N_2}$，都是 N_2 自己的自同态. 由于 N_2 也满足两个链条件，而且 N_2 是不可分解的. 根据 *Fitting* 引理的推论1，每一个 $\rho_2\tau_i|_{N_2}$ 或是幂零的或是自同构. 又因为

$$\rho_2 = \rho_2\tau_1 + \rho_2\tau_2 + \rho_2\tau_3 + \cdots + \rho_2\tau_t$$

$$\rho_2|_{N_2} = 1_{N_2} = (\rho_2\tau_1 + \rho_2\tau_2 + \cdots + \rho_2\tau_t)|_{N_2}$$

根据 *Fitting* 引理的推论2，$\rho_2\tau_i|_{N_2}$不可能都是幂零的. 从而，$\rho_2\tau_1$, $\rho_2\tau_2$, $\cdots$, $\rho_2\tau_t$当中只少有一个是 N_2 的自同构. 但是，$\forall \alpha \in M$，都有

$$\rho_1\tau_1(\alpha) = \tau_1(\alpha) \Longrightarrow \rho_2\tau_1(\alpha) = \rho_2(\rho_1\tau_1(\alpha))$$

$$= \rho_2\rho_1\tau_1(\alpha) = 0$$

即$\rho_2\tau_1 = 0$. 由此可知，$\rho_2\tau_2$, $\rho_2\tau_3$, $\cdots$, $\rho_2\tau_t$中必有N_2的自同构. 不妨认为，$\rho_2\tau_2$是N_2的自同构. 于是，令 $\tau_2(N_2) = \overline{H}_2$,

则有$\rho_2(\overline{H_2})=N_2$，$\overline{H_2}\subseteq H_2$。并且不难知道。$N_2\overset{\tau_2}{\simeq}\overline{H_2}$，

$\overline{H_2}\overset{\rho_2}{\simeq}N_2$。

下面我们指出，$\overline{H}_2=H_2$，为此，令

$$K_2=\{\alpha\in H_2\,|\,\rho_2(\alpha)=0\},$$

它是H_2的一个子模。于是，$\forall\ \alpha\in H_2$，$\rho_2(\alpha)\in N_2$，由$\rho_2\tau_2$是N_2的自同构，则有$\beta\in N_2$，使$\rho_2(\alpha)=\rho_2\tau_2(\beta)$，即$\rho_2(\alpha-\tau_2(\beta))=0$，这样，元素$\alpha$便可写成

$$\alpha=[\alpha-\tau_2(\beta)]+\tau_2(\beta),$$

其中$\alpha-\tau_2(\beta)\in K_2$，$\tau_2(\beta)\in\overline{H}_2$。这说明，$H_2$是子模$K_2$与$\overline{H}_2$的和，即$H_2=K_2+\overline{H}_2$。并且，如果$\alpha\in K_2\cap\overline{H}_2$，由$\rho_2$是$\overline{H}_2$与$N_2$的同构映射，从而可知$\alpha=0$。这样就有$H_2=K_2\oplus\overline{H}_2$。然而$H_2$是不可分解的。而且$N_2\overset{\tau_2}{\simeq}\overline{H}_2$，可见$\overline{H}_2\neq\{0\}$。从而必有$K_2=\{0\}$，即得$H_2=\overline{H}_2$，亦即$N_2\overset{\tau_2}{\simeq}H_2$，$H_2\overset{\rho_2}{\simeq}N_2$。

为了说明可用H_2替换$M=H_1\oplus N_2\oplus N_3\oplus\cdots\oplus N_s$中的$N_2$，令$M''=H_1+H_2+N_3+\cdots+N_s$，因为$\rho_2(H_1+N_3+\cdots+N_s)=\{0\}$，而且$H_2\overset{\rho_2}{\simeq}N_2$。可知$H_2\cap(H_1+N_3+\cdots+N_s)=\{0\}$从而有

$$M''=H_2\oplus(H_1+N_3+\cdots+N_s)=H_1\oplus H_2\oplus N_3\oplus\cdots\oplus N_s.$$

于是，令

$$\varphi:\alpha_1+\alpha_2+\alpha_3+\cdots+\alpha_s\longmapsto\alpha_1+\tau_2(\alpha_2)+\alpha_3+\cdots+\alpha_s,$$

其中$\alpha_1\in H_1$，$\alpha_i\in N_i(i=2,\ \cdots,\ s)$。

那么，容易知道φ是$M=H_1\oplus N_2\oplus N_3\oplus\cdots\oplus N_s$到子模$M''$的同构。即$\varphi$是$M$的一个自同态，而且$\varphi$是单的。这样，根据命题1，可知$\varphi$是$M$的自同构，从而$\varphi$是满的，故有$M''=M$，即

$$M = H_1 \oplus H_2 \oplus N_3 \oplus \cdots \oplus N_s.$$

照这样继续做下去．由于 $s \leqslant t$，进行完第 s 次替换之后，即有

$$M = H_1 \oplus H_2 \oplus \cdots \oplus H_s$$

由此可见，必定是 $s = t$。到此，总观以上推理过程，定理所要求的两个方面的结论已经完全被证明了．▌

推论 在定理的前提下，则有 $s = t$，并且适当编排 $H_i(i = 1, 2, \cdots, s)$ 的顺序之后，存在M的一个自同构 μ，使得 $\mu(N_i) = H_i$，$i = 1, 2, \cdots, s$。

事实上，由定理的证明过程可知，存在M的一组自同态 μ_1，μ_2，$\cdots$，μ_s，使得

$$N_1 \overset{\mu_1}{\simeq} H_1, \quad N_2 \overset{\mu_2}{\simeq} H_2, \quad \cdots, \quad N_s \overset{\mu_s}{\simeq} H_s.$$

于是，令

$$\mu: \alpha_1 + \alpha_2 + \cdots + \alpha_s \longmapsto \mu_1(\alpha_1) + \mu_2(\alpha_2) + \cdots + \mu_s(\alpha_s),$$

其中 $\alpha_i \in N_i (i = 1, 2, \cdots, s)$。那么，不难指出，$\mu$ 是 M 的自同构，且使$\mu(N_i) = H_i$，$i = 1, 2, \cdots, s$。▌

习　　题

1．设 M，N 都是 R—模，$M \neq \{0\}$，N 不可分解．如果 $\sigma: M \longrightarrow N$，$\tau: N \longrightarrow M$是$R$—同态，使$\tau\sigma$是$M$的一个自同构，那么 σ，τ 都是R—同构．

2．设R—模M满足子模的两个链条件．σ 是 M的一个自同态，于是存在 r，s，使

$$M \supset \sigma(M) \supset \sigma^2(M) \supset \cdots \supset \sigma^{r-1}(M) \supset \sigma^r(M) = \sigma^{r+1}(M) = \cdots,$$

$$\{0\} \subset ker\sigma \subset ker\sigma^2 \subset \cdots \subset ker\sigma^{s-1} \subset ker\sigma^s = ker\sigma^{s+1} = \cdots.$$

证明：$r=s$。

3．设$\sigma_1, \sigma_2, \cdots, \sigma_r$与$\tau_1, \tau_2, \cdots, \tau_s$是$R$—模$M$的两组完全的正交射影，且$\sigma_i \neq 0$，$\tau_j \neq 0$（$i=1, 2, \cdots, r$；$j=1, 2, \cdots, s$）。证明：

（1）$r=s$

（2）在适当编排$\tau_1, \tau_2, \cdots, \tau_r$的顺序之后，有模$M$的自同构$\mu$，使得$\tau_i=\mu^{-1}\sigma\ \mu(i=1, 2, \cdots, r)$．

4．设R—模M有直和分解式：$M=M_1\oplus M_2\oplus\cdots\oplus M_n$，其中$M_i$都不可分解，且$M_1\simeq M_i(i=1, 2, \cdots, r)$．证明：如果$\sigma$，$\sigma'$都是模$M$的射影，使$\sigma(M)$，$\sigma'(M)$都是不可分解的．那么存在$M$的自同构$\mu$，使$\sigma'=\mu^{-1}\sigma\mu$。

5．设R—模M满足子模的两个链条件．σ是M的自同态．证明：如果$M=M_0\oplus M_1$，使得$\sigma|_{M_0}$是幂零的，$\sigma|_{M_1}$是自同构，那么这样的M_0与M_1是唯一确定的。

6．设σ，τ都是R—模M的射影．证明：

（1）$Im\sigma=Im\tau \Longleftrightarrow \sigma\tau=\tau$，$\tau\sigma=\sigma$。

（2）$ker\sigma=ker\tau \Longleftrightarrow \sigma\tau=\sigma$，$\tau\sigma=\tau$。

7．设R—模M满足子模的两个链条件．令其高$h(M)=r$，由Krull—Schmidt定理，存在项数一定的直和分解式：

$$M=M_1\oplus M_2\oplus\cdots\oplus M_s，M_i都是不可分解的。$$

可以称s为模M的长，记作$l(M)=s$。试问：模M的这两个数量特征有何关系？是否一定$h(M)=l(M)$？

8．设R—模M满足子模的两个链条件．令$M=M_1\oplus M_2\oplus\cdots\oplus M_r$，$M_i$都是不可分解的．证明：如果$M=N_1\oplus N_2\oplus\cdots\oplus N_r$，$N_j\neq\{0\}$，$j=1, 2, \cdots, r$．那么$N_j$也都是不可分解的。

9．证明：如果R—模M满足子模的降链条件，那么M可以分解成有限个不可分解的子模的直和。

第2章

主理想环上的有限生成模

本章讨论有限生成模的结构以及有限生成模的自同态的基本性质。

我们知道，R—模M是有限生成的当且仅当M可表成有限个循环子模的和：

$$M = Rx_1 + Rx_2 + \cdots + Rx_s$$

当然，一般来说上述的和未必是直和，因而模M的结构尚不能由各个循环子模Rx_i的结构所唯一决定。本章的主要结果将指出，如果R是主理想环，那么上述有限生成模M的表示式可以改善成为直和：

$$M = Rz_1 \oplus Rz_2 \oplus \cdots \oplus Rz_r$$

并且此和式具有某种意义下的唯一性。

正如大家所熟悉的，在有限维线性空间及其线性变换的理论中，域上的矩阵起了决定性的作用。在以下关于有限生成模的讨论中，交换环（特别是主理想环）上的矩阵及行列式将是分析问题与解决问题的重要工具。为了叙述上的整齐起见，我们把所需要的关于矩阵及行列式的一些内容集中起来放在本章开头，做为一节来讲。

§1 交换环上的矩阵与行列式

在这一节里讲以下三个问题：

1．一般环上的矩阵概念及其运算性质．

2．交换环上的行列式概念与基本性质．

3．矩阵的相抵关系；主理想环上矩阵在相抵关系之下的标准形．

我们已经熟悉数域以及一般域上矩阵的概念及其基本运算性质．这里我们首先把它们推广到一般的环上去．

设R为任意的环，m与n为任意的两个正整数．于是，对于任意取自环R中的$m\times n$个（当然可以有重复的）元素a_{ij}，把它们排列成以下形式：

$$\begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \cdot & \cdot & \cdots & \cdot \\ a_{m1} & a_{m2} & \cdots & a_{mn} \end{pmatrix} \qquad (1)$$

则称排列成这种形式的$m\times n$个元素a_{ij}是环R上的一个$m\times n$矩阵．通常把矩阵（1）简记成

$$(a_{ij}),\quad a_{ij}\in R,\ i=1,\ 2,\ \cdots,\ m;\ j=1,\ 2,\ \cdots,\ n$$

或者是

$$(a_{ij})_{m\times n},\qquad a_{ij}\in R$$

一般用大写的拉丁字母来表示一个矩阵，例如，

$$A=(a_{ij})_{m\times n},\quad X=(x_{ij})_{p\times q}$$

等等．

环R上的两个$m\times n$矩阵$A=(a_{ij})_{m\times n}$与$B=(b_{ij})_{m\times n}$当且仅

当对于每一对 i 与 $j(1\leqslant i\leqslant m;\ 1\leqslant j\leqslant n)$ 都有

$$a_{ij}=b_{ij}$$

时，则称 A与 B 是相等的矩阵，记作$A=B$。

对于环 R上的m×n矩阵$A=(a_{ij})_{m\times n}$，称

$$a_{ij};\quad 1\leqslant i\leqslant m,\ 1\leqslant j\leqslant n$$

为 A 的 i，j 位置的元素，简称为$(i,\ j)$元素。因而，$A=B\Longleftrightarrow$ $(i,\ j)$ 元素完全都相等。

称 $A=(a_{ij})_{m\times n}$中的元素

$$a_{i1},\ a_{i2},\ \cdots,\ a_{in},\ 1\leqslant i\leqslant m,$$

为 A 的第 i 行元素，简称为 A 的第 i 行；而称

$$a_{1j},\ a_{2j},\ \cdots,\ a_{mj},\ 1\leqslant j\leqslant n,$$

为 A 的第 j 列元素，简称为 A 的第 j 列。这样，每一个mxn矩阵 $A=(a_{ij})_{m\times n}$都有m个行与n个列。其中每一个行

$$a_{i1},\ a_{i2},\ \cdots,\ a_{in}$$

都可以看成环 R 上的一个 n 元向量，即 $R^{(n)}$ 中的一个元素；而每一个列

$$a_{1j},\ a_{2j},\ \cdots,\ a_{mj}$$

都可以看成环 R 上的一个 m 元向量，即 $R^{(m)}$ 中的一个元素。因此又可以说，$A=(a_{ij})_{m\times n}$与$B=(b_{ij})_{m\times n}$相等$\Longleftrightarrow A$与B的 m 个行向量依次是相等的$\Longleftrightarrow A$与B 的 n 个列向量依次是相等的。

考虑环 R 上一切m×n矩阵组成的集合。令

$$M_{m\times n}(R)=\{(a_{ij})\,|\,a_{ij}\in R;\ 1\leqslant i\leqslant m,\ 1\leqslant j\leqslant n\}$$

在$M_{m\times n}(R)$中规定加法运算如下：

$$(a_{ij})+(b_{ij})=(a_{ij}+b_{ij});$$

R 与 $M_{m\times n}(R)$到$M_{m\times n}(R)$的左（右）倍数乘法如下：

$$r(a_{ij})=(ra_{ij})\quad ((a_{ij})r=(a_{ij}r))$$

其中 (a_{ij})，$(b_{ij})\in M_{m\times n}(R)$，$r\in R$。

进而，对任一 $(a_{is})\in M_{m\times n}(R)$与任意一$(b_{sj})\in M_{n\times p}(R)$规定乘法如下：

$$(a_{ik})(b_{kj})=(c_{ij}),$$

其中

$$c_{ij}=a_{i1}b_{1j}+a_{i2}b_{2j}+\cdots+a_{in}b_{nj}$$
$$=\sum_{k=1}^{n}a_{ik}b_{kj}$$

因此，$(c_{ij})\in M_{m\times p}(R)$．从而上述之乘法是 $M_{m\times n}(R)$ 与 $M_{n\times p}(R)$ 到 $M_{m\times p}(R)$ 的一个运算．特别地，当 $m=p=n$时，这就是 $M_{n\times n}(R)$ 的一个乘法运算．$M_{n\times n}(R)$ 中的每一个矩阵 $A=(a_{ij})_{n\times n}$其行数与列数相等，都等于 n．通常把这样的矩阵叫做 n 阶方阵．

对于环R上的一切n阶方阵做成的集合简记为$M_n(R)$．按上述的规定，$\{M_n(R);\ +,\ \cdot\}$ 就成了有两个代数运算：加法与乘法的代数体系．并且还有一个 R 与 $M_n(R)$ 到$M_n(R)$ 的倍数乘法．进而不难指出如下简单的，重要的结果，即有

定理 1 设R为环．则有

（1） $\{M_{m\times n}(R);\ +\}$ 是交换群．

（2）如果环 R 有恒等元素，那么加法群 $M_{m\times n}(R)$ 做成环 R上的左（右）模，并且是有限生成的．

（3） $\{M_n(R);\ +,\ \cdot\}$ 是环，叫做 R上的 n 阶全阵环．如果环 R有恒等元素，那么 n 阶全阵环$M_n(R)$ 也有恒等元素，即通常所说的 n 阶单位矩阵

$$\begin{pmatrix} 1 & 0 & 0 & \cdots & 0 \\ 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \cdots & 0 \\ \cdot & \cdot & \cdot & \cdots & \cdot \\ 0 & 0 & 0 & \cdots & 1 \end{pmatrix}$$

为环 $M_n(R)$ 的恒等元素．▌

定理 1 中的所有结论都是我们所熟知的．它的证明与数域的情形没有什么不同．其中加法群

$$\{M_{m\times n}(R);\ +\}$$

的零元素就是所谓的零矩阵——所有元素都是零的矩阵。记作$O_{m\times n}$，或简记为O。$M_{m\times n}(R)$ 中的任一元素$A=(a_{ij})$ 的负元素为矩阵 $(-a_{ij})$，即 $-(a_{ij}) = (-a_{ij})$。

一个mxn矩阵$A=(a_{ij})_{m\times n}$，如果对于$i\neq j$时$a_{ij}=0$，则称$A=(a_{ij})$ 为对角形阵，简记为

$$A=diag\{a_{11},\ a_{22},\ \cdots,\ a_{mm}\}\quad (m\leqslant n).$$

当A 为方阵时，n 阶对角形阵有以下形式

$$A=\begin{pmatrix} a_1 & 0 & 0 & \cdots & 0 \\ 0 & a_2 & 0 & \cdots & 0 \\ 0 & 0 & a_3 & \cdots & 0 \\ \cdot & \cdot & \cdot & \cdots & \cdot \\ 0 & 0 & 0 & \cdots & a_n \end{pmatrix}=diag\{a_1,\ a_2,\ \cdots,\ a_n\}$$

特别地，如果对角形方阵

$$A=diag\{a_1,\ a_2,\ \cdots,\ a_n\}$$

的对角线上诸元素均相同，即 $a_1=a_2=\cdots a_n=a$，这时就说A为纯量阵。不难指出，$M_n(R)$ 中一切纯量阵做成的子集 C 是全阵环$M_n(R)$ 的一个子环，并且与环 R 是同构的，即有

$$\varphi:\ a\longmapsto diag\{a,\ a,\ \cdots,\ a\}$$

是R与C的一个同构映射：

$$R\cong C.$$

据此，我们总可以认为环 R 是全阵环$M_n(R)$ 的子环。特别地，当$n=1$时，$R=M_1(R)=\{(a)\mid a\in R\}$.

一般来说，除非R为零环，只要 $n>1$，全阵环 $M_n(R)$ 必有真零因子；只要R不是零乘环，当$n>1$时，$M_n(R)$ 决不是交换环。

再有，把一个$m\times n$矩阵A的各行依次做为列，得到一个确定的$n\times m$矩阵，叫做矩阵 A 的**转置矩阵**，记作 A'。显然可见，$(A')'=A$。当 R为交换环时，以下熟知的规则也是成立的。即

有

$$(AB)' = B'A'$$

此处只要 A与 B是可乘的就行，并且不难推广到任意有限个矩阵的情形。

最后说明一下可逆矩阵的概念。设 R为有恒等元素的环，从而全阵环 $M_n(R)$ 也有恒等元素，即 n 阶单位矩阵

$$E = \begin{pmatrix} 1 & 0 & 0 & \cdots & 0 \\ 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \cdots & 0 \\ \cdot & \cdot & \cdot & \cdots & \cdot \\ 0 & 0 & 0 & \cdots & 1 \end{pmatrix}$$

于是，

$$EA = A = AE, \qquad A \in M_n(R).$$

如果对于$A \in M_n(R)$，存在$B \in M_n(R)$，使得

$$AB = E = BA,$$

则称A是**可逆的**，同时称B为A的**逆阵**。容易验证，一个阵 A，如果有逆矩阵为B，那么该逆矩阵是唯一的。从而可记作$B = A^{-1}$。即有

$$AA^{-1} = E = A^{-1}A.$$

显然，可逆矩阵必不是零矩阵，然而一个非零矩阵则未必是可逆的。如果A，$B \in M_n(R)$ 都是可逆的，那么A与B的积 AB也是可逆的，并且

$$(AB)^{-1} = B^{-1}A^{-1}.$$

若令

$$GL_n(R) = \{ A \in M_n(R) \mid A\text{可逆} \},$$

可知$GL_n(R)$ 是乘法半群 $\{ M_n(R); \cdot \}$ 的一个子群，叫做 R上的 n 阶**完全线性群**。

为了后面讨论问题的需要，我们把行列式的概念推广到一般的交换环上去。

我们回顾一下，在高等代数中关于行列式概念的定义。

设 F 为任一数域，所谓数域 F 上的一个 n阶行列式是由F中的n^2个数a_{ij}（$1\leqslant i$，$j\leqslant n$）构成的一个代数和：

$$\sum_{i_1 i_2\cdots i_n\in S_n}(-1)^{\tau[i_1 i_2\cdots i_n]}a_{1i_1}a_{2i_2}\cdots a_{ni_n} \qquad (1)$$

其中 $i_1 i_2\cdots i_n$为S_n 中的任一 n 元排列，而 $\tau[i_1 i_2\cdots i_n]$ 则是排列 $i_1 i_2\cdots i_n$的反序数。代数和（1）的结果是数域 F 中的一个确定的数，叫做这个 n 阶行列式的值。并记作

$$\begin{vmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \cdot & \cdot & \cdots & \cdot \\ a_{n1} & a_{n2} & \cdots & a_{nn} \end{vmatrix} = \sum_{i_1 i_2\cdots i_n\in S_n}(-1)^{\tau(i_1 i_2\cdots i_n)}a_{1i_1}a_{2i_2}\cdots a_{ni_n}$$

明显可见，这样定义的 n 阶行列式实际上可以认为是定义在n阶方阵集合$M_n(F)$ 上的一个函数，其值域为 F。并且由行列式的基本性质（这种函数的基本规律）可以看出，这个函数的基本特性是以做为自变量的 n 阶矩阵的行（或列）为“要素”来加以刻划的。这就启发我们，如果把 n 阶方阵的每一行（列）看成n维线性空间$F^{(n)}$（这是一个特殊的有限生成模）中的一个向量，那么 n 阶行列式就可以认为是定义在$F^{(n)}$上的，在F中取值的一个 n 元函数。这样来理解 n 阶行列式的概念不仅是自然的，而且是可取的。基于这样的想法，我们把数域 F上的 n 阶行列式概念推广到一般的R—模 $R^{(n)}$ 的情形，此处R是任意的有恒等元素的交换环。

设 R 为有恒等元素的交换环。M_1，M_2，…，M_r 与N均为 R 上的模。而

$$P=M_1\oplus M_2\oplus\cdots\oplus M_r$$

考虑P到N的一个映射（也叫定义在P上，在N中取值的函数）：

$$f:\ P=M_1\oplus M_2\oplus\cdots\oplus M_r\longrightarrow N,$$

$$f:(\alpha_1, \alpha_2, \cdots, \alpha_r) \longmapsto \beta,$$

或

$$f(\alpha_1, \alpha_2, \cdots, \alpha_r)=\beta,$$

其中$\alpha_i \in M_i$，$\beta \in N$，$i=1, 2, \cdots, r$。

如果对任意的k，$l \in R$，α'，$\alpha'' \in M_i$，均有

$$\begin{aligned} & f(\alpha_1, \cdots, \alpha_{i-1}, k\alpha'+l\alpha'', \alpha_{i+1}, \cdots, \alpha_r) \\ = & kf(\alpha_1, \cdots, \alpha_{i-1}, \alpha', \alpha_{i+1}, \cdots, \alpha_r)+ \\ & lf(\alpha_1, \cdots, \alpha_{i-1}, \alpha'', \alpha_{i+1}, \cdots, \alpha_r), \end{aligned}$$

则称 f 是 r **重线性映射**（函数），$i=1, 2, \cdots, r$。

特别地，当$N=R$时，称 r 重线性映射 f 为 r **重线性型**。而当$N=R$，$M_1=M_2=\cdots=M_r=M$ 时，则称 f 为**模M上的 r 重线性型**。

设 f 为 R—模 M上的 r 重线性型，即

$$f: M^{(r)} \longrightarrow R,$$

$$f:(\alpha_1, \alpha_2, \cdots, \alpha_r) \longmapsto a,$$

其中$\alpha_i \in M(i=1, 2, \cdots, r)$，$a \in R$，使得

$$f(\cdots, k\alpha'+l\alpha'', \cdots)=kf(\cdots, \alpha', \cdots)+lf(\cdots, \alpha'', \cdots)$$

对任意的$k, l \in R$；α'，$\alpha'' \in M$。

如果对任一置换 $\sigma \in S_r$，均有

$$\begin{aligned} & \sigma f(\alpha_1, \alpha_2, \cdots, \alpha_r) \equiv f(\alpha_{\sigma(1)}, \alpha_{\sigma(2)}, \cdots, \alpha_{\sigma(r)}) \\ = & f(\alpha_1, \alpha_2, \cdots, \alpha_r), \end{aligned}$$

则称 f 为模 M上对称的 r 重线性映射。

如果对任一置换$\sigma \in S_r$，均有

$$f(\alpha_{\sigma(1)}, \alpha_{\sigma(2)}, \cdots, \alpha_{\sigma(r)})=sgn\sigma f(\alpha_1, \alpha_2, \cdots, \alpha_r).$$

则称 f 为模 M 上反对称的 r 重线性映射，其中 $sgn\sigma$是置换 σ的符号，规定为$sgn\sigma=(-1)^t$，t 为置换 σ 的反序数。

如果，当 $i \neq j$ 而 $\alpha_i=\alpha_j$时，均有

$$f(\alpha_1, \cdots \alpha_i, \cdots, \alpha_j, \cdots, \alpha_r)=0,$$

则称 f 为模M上交错的 r 重线性映射。

例 1 令 $M=(F^{(n)})^{(n)}=F^{(n)}\oplus F^{(n)}\oplus\cdots\oplus F^{(n)}$，$F$ 为任一数域。而映射

$$f: M\longrightarrow F,$$

$$f: (\alpha_1,\alpha_2,\cdots,\alpha_n)\longmapsto a,$$

其中

$$\alpha_1=(a_{11},\ a_{12},\ \cdots,\ a_{1n}),$$

$$\alpha_2=a_{21},\ a_{22},\ \cdots,\ a_{2n}),$$

$$\vdots$$

$$\alpha_n=(a_{n1},\ a_{n2},\ \cdots,\ a_{nn}),$$

$$a=\begin{vmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \cdot & \cdot & \cdots & \cdot \\ a_{n1} & a_{n2} & \cdots & a_{nn} \end{vmatrix}=|A|,\ A=(a_{ij})$$

即 a 是以 α_1，α_2，$\cdots$，α_n 依次做行得到的 n 阶方阵 A 的行列式之值。

不难验证，映射 f 是 F—模 $F^{(n)}$ 上反对称的、交错的 n 重线性型。

例 2 令 $M=R^{(2)}=\{(a,\ b)|a,\ b\in R\}$，$R$为任一有恒等元素的交换环。而映射

$$f: M^{(2)}=R^{(2)}\oplus R^{(2)}\rightarrow R,$$

$$f: ((a_{11},\ a_{12}),\ (a_{21},\ a_{22}))\longmapsto a_{11}a_{22}-a_{12}a_{21}$$

于是容易验证映射 f 是R—模 $R^{(2)}$ 上反对称的交错的 2 重线性型。2 重线性型通常也叫做双线性型。

定理 2 设 R为有恒等元素的交换环。M与 N均为 R—模。令 f 为M上的任一 r 重线性映射。则有，如果f 是交错的那么f必为反对称的。

证 首先考虑 σ 是一个对换的特殊情形。令 $\sigma=(ij)$，去证

$$\sigma f(\alpha_1,\cdots,\alpha_i,\cdots,\alpha_j,\cdots,\alpha_r)=\mathrm{sgn}\sigma f(\alpha_1,\cdots,\alpha_i,\cdots,\alpha_j,\cdots,\alpha_r),$$

即

$$f(\alpha_1,\cdots,\alpha_{\sigma(i)},\cdots,\alpha_{\sigma(j)},\cdots,\alpha_r)$$
$$=-f(\alpha_1,\cdots,\alpha_i,\cdots,\alpha_j,\cdots,\alpha_r)$$

取$\alpha_i=\alpha_i'+\alpha_i''$, $\alpha_j=\alpha_i'+\alpha_i''$. 由$f$是交错的，则有

$$\begin{aligned}0&=f(\cdots,\alpha_i'+\alpha_i'',\cdots,\alpha_i'+\alpha_i'',\cdots)\\&=f(\cdots,\alpha_i',\cdots,\alpha_i',\cdots)+f(\cdots,\alpha_i',\cdots,\alpha_i'',\cdots)\\&+f(\cdots,\alpha_i'',\cdots,\alpha_i',\cdots)+f(\cdots,\alpha_i'',\cdots,\alpha_i'',\cdots)\\&=f(\cdots,\alpha_i',\cdots,\alpha_i'',\cdots)+f(\cdots,\alpha_i'',\cdots,\alpha_i',\cdots)\end{aligned}$$

从而

$$f(\cdots,\alpha_i'',\cdots,\alpha_i',\cdots)=-f(\cdots,\alpha_i',\cdots,\alpha_i'',\cdots)$$

即

$$\sigma f(\alpha_1,\cdots,\alpha_i',\cdots,\alpha_i'',\cdots,\alpha_r)=Sgn\sigma f(\cdots,\alpha_i',\cdots,\alpha_i'',\cdots).$$

对于σ是任意的奇（偶）置换的情形，因为σ可以表成奇（偶）数个对换的乘积，所以也有

$$\sigma f(\alpha_1,\alpha_2,\cdots,\alpha_r)=sgn\sigma f(\alpha_1,\alpha_2,\cdots,\alpha_r).$$ ∎

定理 3 设R为任一有恒等元素的交换环，$a\in R$。那么在模$R^{(n)}$上存在唯一的交错的n重线性型：

$$f:(R^{(n)})^{(n)}\longrightarrow R,$$

使得 $f(\varepsilon_1,\varepsilon_2,\cdots,\varepsilon_n)=a$。其中

$$\varepsilon_1=(1,0,0,\cdots,0),$$
$$\varepsilon_2=(0,1,0,\cdots,0),$$
$$\vdots$$
$$\varepsilon_n=(0,0,0,\cdots,1).$$

证 首先证明唯一性，即在模$(R^{(n)})^{(n)}$上至多只能有一个交错的n重线性型f，使得

$$f(\varepsilon_1,\varepsilon_2,\cdots,\varepsilon_n)=a$$

事实上，如果f是模$R^{(n)}$上交错的n重线性型，那么对于任意的$\alpha_1,\alpha_2,\cdots,\alpha_n\in R^{(n)}$，则有

$$\alpha_1=a_{11}\varepsilon_1+a_{12}\varepsilon_2+\cdots+a_{1n}\varepsilon_n,$$

$$\alpha_2 = a_{21}\varepsilon_1 + a_{22}\varepsilon_2 + \cdots + a_{2n}\varepsilon_n$$

$$\vdots$$

$$\alpha_n = a_{n1}\varepsilon_1 + a_{n2}\varepsilon_2 + \cdots + a_{nn}\varepsilon_n$$

其中 $a_{ij} \in R$, $1 \leqslant i, j \leqslant n$, 于是

$$f(\alpha_1, \alpha_2, \cdots, \alpha_n) = f\left(\sum_{j_1=1}^{n} a_{1j_1}\varepsilon_{j_1}, \sum_{j_2=1}^{n} a_{2j_2}\varepsilon_{j_2}, \cdots, \sum_{j_n=1}^{n} a_{nj_n}\varepsilon_{j_n}\right)$$

$$= \sum_{j_1, j_2, \cdots, j_n=1}^{n} a_{1j_1}a_{2j_2}\cdots a_{nj_n} f(\varepsilon_{j_1}, \varepsilon_{j_2}, \cdots, \varepsilon_{j_n}).$$

由于 f 是交错的，所以在上述的和式里只有当 $j_1, j_2, \cdots, j_n$ 彼此不同时才可能有不等于零的项出现。而当 $j_1, j_2, \cdots, j_n$ 彼此不同时，根据定理 2，可知

$$f(\varepsilon_{j_1}, \varepsilon_{j_2}, \cdots, \varepsilon_{j_n}) = (-1)^{\tau(j_1j_2\cdots j_n)} f(\varepsilon_1, \varepsilon_2, \cdots, \varepsilon_n)$$

从而就有

$$f(\alpha_1, \alpha_2, \cdots, \alpha_n) = \sum_{j_1j_2\cdots j_n \in S_n} (-1)^{\tau(j_1j_2\cdots j_n)} a_{1j_1}a_{2j_2}\cdots a_{nj_n} f(\varepsilon_1, \varepsilon_2, \cdots, \varepsilon_n)$$

再由 $f(\varepsilon_1, \varepsilon_2, \cdots, \varepsilon_n) = a$，便得

$$f(\alpha_1, \alpha_2, \cdots, \alpha_n) = \sum_{\sigma \in S_n} \operatorname{sgn}\sigma\, a a_{1\sigma(1)} a_{2\sigma(2)} \cdots a_{n\sigma(n)} \tag{1}$$

$f(\alpha_1, \alpha_2, \cdots, \alpha_n)$ 的这个表成代数和的表达式说明 $f(\alpha_1, \alpha_2, \cdots, \alpha_n)$ 是由 $\alpha_1, \alpha_2, \cdots, \alpha_n$ 与 a 所唯一决定的。即在模 $R^{(n)}$ 上对自然"基元素" $\varepsilon_1, \varepsilon_2, \cdots, \varepsilon_n$ 的值为 a 的交错 n 重线性型 f，如果存在的话，是唯一的，同时 f 可以表成（1）式那样的代数和的形式。

其次指出模 $R^{(n)}$ 上必有交错的 n 重线性型。为此，由唯一性的证明可以想到，只须验证由（1）式所定义的映射 f 必合所求就行了。

事实上明显可见，(1)式确实具体地定义了一个 $(R^{(n)})^{(n)}$

到R的映射f. 为了验证f是线性的，不失一般性，可令

$$\alpha_1' = a_{11}'\varepsilon_1 + a_{12}'\varepsilon_2 + \cdots + a_{1n}'\varepsilon_n,$$
$$\alpha_1'' = a_{11}''\varepsilon_1 + a_{12}''\varepsilon_2 + \cdots + a_{1n}''\varepsilon_n$$

则有

$$\alpha_1' + \alpha_1'' = (a_{11}' + a_{11}'')\varepsilon_1 + (a_{12}' + a_{12}'')\varepsilon_2 + \cdots + (a_{1n}' + a_{1n}'')\varepsilon_n$$

于是，由映射f的定义式（1），可知

$$f(\alpha_1', \alpha_2, \cdots, \alpha_n) = \sum_{\sigma \in S_n} \mathrm{sgn}\sigma a a_{1\sigma(1)}' a_{2\sigma(2)} \cdots a_{n\sigma(n)}$$

$$f(\alpha_1'', \alpha_2, \cdots, \alpha_n) = \sum_{\sigma \in S_n} sgn\sigma a a_{1\sigma(1)}'' a_{2\sigma(2)} \cdots a_{n\sigma(n)}$$

从而对 k, $l \in R$, 可得

$$f(k\alpha_1' + l\alpha_1'', \alpha_2, \cdots, \alpha_n)$$

$$= \sum_{\sigma \in S_n} sgn\sigma a(a_{1\sigma(1)}' + a_{1\sigma(1)}'')a_{2\sigma(2)} \cdots a_{n\sigma(n)}$$

$$= \sum_{\sigma \in S_n} sgn\sigma\, a k a_{1\sigma(1)}' a_{2\sigma(2)} \cdots a_{n\sigma(n)}$$

$$+ \sum_{\sigma \in S_n} sgn\sigma a l a_{1\sigma(1)}'' a_{2\sigma(2)} \cdots a_{n\sigma(n)}$$

$$= kf(\alpha_1', \alpha_2, \cdots, \alpha_n) + lf(\alpha_1'', \alpha_2, \cdots, \alpha_n)$$

这就证明了映射f是模$R^{(n)}$上的n重线性型.

最后，我们还要证明当$i \neq j$而$\alpha_i = \alpha_j$时，$f(\alpha_1 \cdots, \alpha_i, \cdots, \alpha_j, \cdots, \alpha_n) = 0$，即$f$也是交错的. 为了简便，不失一般性，取$i = 1$，$j = 2$. 令$\rho = (12)$. 于是，含有$n!$个元素的$n$阶置换的集合$S_n$就可以分解成$n!/2$个2元子集的并集：

$$S_n = \bigcup_{\sigma \in A_n} \{\sigma, \sigma\rho\}$$

其中A_n为n阶偶置换的集合. 与此相应的，在n重线性型f的定义

式（1）的 $n!$ 个项中，对应于每一个偶置换 $\sigma\in A_n$的项为

$$sgn\sigma a a_{1\sigma(1)}a_{2\sigma(2)}\cdots a_{n\sigma(n)}$$
$$=+a a_{1\sigma(1)}a_{2\sigma(2)}\cdots a_{n\sigma(n)}$$

同时就有唯一的对应于奇置换 $\sigma\rho$ 的项为

$$sgn\sigma\rho\ a\ a_{1\sigma\rho(1)}a_{2\sigma\rho(2)}\cdots a_{n\sigma\rho(n)}$$

由于 $\alpha_1=\alpha_2$，所以 $a_{1\sigma(1)}=a_{2\sigma(1)}$，$a_{1\sigma(2)}=a_{2\sigma(2)}$ 。并且 $\rho(1)=2$，$\rho(2)=1$，$\rho(3)=3$，…，$\rho(n)=n$；$sgn\sigma\rho=-1$，这样则有

$$sgn\sigma\rho\ a\ a_{1\sigma\rho(1)}a_{2\sigma\rho(2)}\cdots a_{n\sigma\rho(n)}$$
$$=-a\ a_{1\sigma(2)}a_{2\sigma(1)}\cdots a_{n\sigma(n)}$$
$$=-a\ a_{1\sigma(1)}a_{2\sigma(2)}\cdots a_{n\sigma(n)}$$

由此可见，在映射 f 的定义式(1) 中的 $n!$ 个项是两两相抵消的。从而即得

$$f(\alpha_1,\alpha_2,\cdots,\alpha_n)=0,\ \alpha_1=\alpha_2$$

这样，又证明了 n 重线性型 f 也是交错的。同时明显可见，由（1）式所定义的映射 f，使得

$$f(\varepsilon_1,\varepsilon_2,\cdots,\varepsilon_n)=a$$

总之，模 $R^{(n)}$ 上使得 $f(\varepsilon_1,\varepsilon_2,\cdots,\varepsilon_n)=a$的交错 n 重线性型是存在的，并且可以表达成形如（1）式的和。∎

由于$R^{(n)}$中的元素都是环R上的n元序列，从而$(R^{(n)})^{(n)}$中的元素 $(\alpha_1,\alpha_2,\cdots,\alpha_n)$ 恰好确定一个 R 上的 n 阶方阵：

$$A=\begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n}\\ a_{21} & a_{22} & \cdots & a_{2n}\\ \cdot & \cdot & \cdots & \cdot\\ a_{n1} & a_{n2} & \cdots & a_{nn}\end{pmatrix}$$

其中 $\alpha_i=(a_{i1},\ a_{i2}\ ,\ \cdots,\ a_{in})$，$i=1,\ 2,\ \cdots,\ n$ 。并且对于 $M_n(R)$ 中的每一 n 阶方阵 $A=(a_{ij})$ ，也都存在 $(R^{(n)})^{(n)}$ 中的一个元素 $(\alpha_1,\ \alpha_2,\ \cdots,\ \alpha_n)$，使其按上述方式（以$\alpha_i$的分量做为第 i 行）所确定的方阵就是已给的 n 阶方阵 $A=(a_{ij})$ 。确

切地说，就是在映射φ之下：

$$\varphi:\ (a_1,\ a_2,\ \cdots,\ a_n)\ \longmapsto A=(a_{ij})$$

其中 $a_i=(a_{i1},\ a_{i2},\ \cdots,\ a_{in})$，$i=1,\ 2,\ \cdots,n$，$(R^{(n)})^{(n)}$与$M_n(R)$是模同构的。因此，模 $R^{(n)}$ 上的任意一个 n 重线性型 f 均可认为是 $M_n(R)$ 上的线性型，此时其变元自然被理解为n阶方阵的行。这样，根据定理3，我们就有了定义n阶行列式概念的依据。

定义 设R为有恒等元素的交换环。我们把定义在$M_n(R)$上并且满足

$$d(I_n)=1_R\ \ (I_n\text{为}\ n\ \text{阶单位阵})$$

的交错的、n 重线性型 d 叫做是 M_n(R) 上的行列式函数。而把元素$d(A)\in$R叫做是n阶方阵A的行列式，并且记作$d(A)=|A|$或$d(A)=|a_{ij}|$，$A=(a_{ij})$。

容易看出，高等代数中定义的n阶行列式是上述行列式定义的一个特殊情形。并且，正如下面将要指出的那样，在高等代数中讲到的n阶行列式的一些基本性质对上面定义的一般行列式来说，多数都是成立的。

定理 4 设R为有恒等元素的交换环，A与B为任二n阶方阵。则有

(1) 模$M_n(R)$上的每一个交错的n重线性型f均是$M_n(R)$上行列式函数d的“常数”倍，即

$$f=ad,\ a\in R$$

并且这个a是唯一确定的。

(2) $M_n(R)$上的行列式函数d可以表成如下的$n!$项的代数和：

$$d(A)=\sum_{\sigma\in S_n}sgn\sigma\ a_{1\sigma(1)}a_{2\sigma(2)}\cdots a_{n\sigma(n)}$$

或者

$$|A|=\sum_{j_1 j_2\cdots j_n\in S_n}(-1)^{\tau(j_1 j_2\cdots j_n)}a_{1j_1}a_{2j_2}\cdots a_{nj_n}$$

其中 $j_1 j_2\cdots j_n$ 是$\begin{pmatrix}1 & 2 & \cdots & n\\ j_1 & j_2 & \cdots & j_n\end{pmatrix}$的简写，而 $\tau[j_1\ j_2\ \cdots j_n]$ 为 $j_1 j_2\cdots j_n$的反序数；$A=(a_{ij})$.

（3） $|A'|=|A|$

（4） $|AB|=|A|\cdot|B|$

（5）如果 A是可逆矩阵，那么$|A|$是R中的可逆元素。

（6）如果 A与B 相似，即 $B=PAP^{-1}$，那么$|A|=|B|$.

证　令 f 为 $M_n(R)$上的任意一个交错的 n 重线性型，使得 $f(I_n)=a$，I_n 为 n 阶单位阵。

于是，容易验证映射

$$ad:\ M_n(R)\longrightarrow R,$$

$$ad:\ A\longmapsto ad(A),$$

是模$M_n(R)$ 上的一个交错的 n 重线性型，并且使得

$$ad(I_n)=a$$

从而由定理 3 的唯一性结果，可知

$$f=ad$$

由此，同时也就表明了 a 的唯一性。这样，（1）被证明了。

（2）只是定理 3 的存在性对于 $f(I_n)=1_R$ 的特殊情形。这里为了更加突出起见又重新强调一遍就是了。

（3）令 $A=(a_{ij})$ ，$A'=(c_{ij})$ ，则有 $a_{ij}=c_{ji}$。由于 R 是交换环，所以每一个乘积

$$a_{i_1 1}a_{i_2 2}\cdots a_{i_n n}$$

均可写成

$$a_{1j_1}a_{2j_2}\cdots a_{nj_n}$$

于是，如果σ是置换：$\sigma(k)=i_k$，那么σ^{-1}是置换：$\sigma^{-1}(k)=j_k$.

这样就有

$$|A'|=\sum_{\sigma\in S_n} sgn\sigma c_{1\sigma(1)}c_{2\sigma(2)}\cdots c_{n\sigma(n)}$$

$$=\sum_{\sigma\in S_n} sgn\sigma a_{\sigma(1)1}a_{\sigma(2)2}\cdots a_{\sigma(n)n}$$

$$=\sum_{\sigma^{-1}\in S_n} sgn\sigma^{-1}a_{1\sigma^{-1}(1)}a_{2\sigma^{-1}(2)}\cdots a_{n\sigma^{-1}(n)}$$

$$=|A|$$

（4）我们考虑模 $M_n(R)$ 上的一个映射：

f：$M_n(R)\longrightarrow R$,

f：$C\longmapsto|CB|$。

我们注意到：如果 n 阶方阵 C 的行依次为 α_1，α_2，…，α_n；而 β_1，β_2,…,β_n 依次为 n 阶方阵 B 的列，那么乘积 CB 的第 i 行就是

$$\alpha_i\beta_1,\ \alpha_i\beta_2,\ \cdots,\ \alpha_i\beta_n.$$

据此不难验证上述之映射 f 是 $M_n(R)$ 上的一个交错的 n 重线性型。于是由刚证明的（1），则有

$$f=ad,$$

其中 d 为 $M_n(R)$ 上的行列式函数，a 是由 f 所唯一决定的 R 中元素。

这样就有，$\forall C\in M_n(R)$

$$|CB|=f(C)=ad(C)=a|C|.$$

特别地，$|B|=|I_nB|=a|I_n|=a$。从而便得

$$|AB|=a|A|=|B|\cdot|A|=|A|\cdot|B|$$

（5）如果 A 是可逆矩阵，则有 $AA^{-1}=I_n$。于是，由（4）则有

$$|A|\cdot|A^{-1}|=|AA^{-1}|=|I_n|=1_R,$$

可知 $|A|$ 为环 R 中的可逆元素。

（6）如果A与B相似，则有$B=PAP^{-1}$。从而，由（4）以及R为交换环，便得

$$|B|=|PAP^{-1}|=|P|\cdot|A|\cdot|P^{-1}|=|A|.\ \blacksquare$$

定理 5 设R为有恒等元素的交换环。则有

（1）如果n阶方阵B是由交换A的两行（列）而得到的，那么

$$|B|=-|A|.$$

（2）如果n阶方阵B是把A的某一行（列）乘以k而得到的，$k\in R$，那么

$$|B|=k|A|.$$

（3）如果n阶方阵B是把A的第i行（列）的某个倍数加到第j行（列）上而得到的$(i\neq j)$，那么

$$|B|=|A|.$$

（4）如果$A=(a_{ij})$是三角形矩阵，即

$$A=\begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ 0 & a_{22} & \cdots & a_{2n} \\ \cdot & \cdot & \cdots & \cdot \\ 0 & 0 & \cdots & a_{nn} \end{pmatrix}$$

或者

$$A=\begin{pmatrix} a_{11} & 0 & \cdots & 0 \\ a_{21} & a_{22} & \cdots & 0 \\ \cdot & \cdot & \cdots & \cdot \\ a_{n1} & a_{n2} & \cdots & a_{nn} \end{pmatrix}$$

那么$|A|=a_{11}a_{22}\cdots a_{nn}$。

证 令$\alpha_1, \alpha_2, \cdots, \alpha_n$是$n$阶方阵$A$的$n$个行。因为行列式函数$d$是交错的，由定理2可知$d$是反对称的。这样，如果$B$是交换$A$的$i$与$j$两行而得到的$n$阶方阵，则有

$$\begin{aligned}|B|&=d(\alpha_1,\cdots,\alpha_j,\cdots\alpha_i,\cdots,\alpha_n)\\&=-d(\alpha_1,\cdots,\alpha_i,\cdots,\alpha_j,\cdots,\alpha_n)=-|A|\end{aligned}$$

即（1）成立。

（2）是行列式函数 d 的线性性质的特殊情形。下面证明（3）成立。令 n 阶方阵 B是把 A的第 i 行的 k 倍加于第 j 行上而得到的（$i<j$），则有

$$
\begin{aligned}
|B| &= d(\cdots,\alpha_i,\cdots,k\alpha_i+\alpha_j,\cdots)\\
&= kd(\cdots,\alpha_i,\cdots,\alpha_i,\cdots)+d(\cdots,\alpha_i,\cdots,\alpha_j,\cdots)\\
&= d(\cdots,\alpha_i,\cdots,\alpha_j,\cdots)=|A|
\end{aligned}
$$

最后证明（4）成立。由 A是三角形阵，可知

$a_{ij}=0$，当 $j<i$；

或者　$a_{ij}=0$，当 $j>i$。

这样，对任意置换 $\sigma\neq(1)$ 时，必有 $a_{1\sigma(1)}a_{2\sigma(2)}\cdots a_{n\sigma(n)}=0$，从而

$$|A|=\sum_{\sigma\in S_n}sgn\sigma a_{1\sigma(1)}a_{2\sigma(2)}\cdots a_{n\sigma(n)}=a_{11}a_{22}\cdots a_{nn}\qquad\blacksquare$$

定理5所指出的行列式性质表明，可以通过行列式的变换来简化行列式的计算。特别地，如果 R是域，那么对于每一个 n 阶方阵 A 来说，它的行列式 $|A|$ 都可以直接归结为一个三角形矩阵的行列式去计算出来。这其实是高等代数中的一个重要事实。再有，不论在理论上或应用上都很重要的展开定理，对这里定义的一般行列式来说也是成立的。为了指出这个事实，我们需要做如下的一些准备。

设 A为环 R（有恒等元素、交换）上的m×n矩阵。对任意一个k：$1\leqslant k\leqslant m$；$1\leqslant k\leqslant n$，那么由A的 k个行与 k 个列的交叉位置处的k^2个元素（按它们在 A中的位置顺序）做成一个 k 阶方阵T，把 k 阶行列式 $|T|$ 叫做矩阵A的一个k阶子式。特别地，当A是n阶方阵时，A中去掉子式T所在的k行与k列之后，余下的 $n-k$个行与 $n-k$ 个列顺便也产生A的一个 $n-k$ 阶子式 $|\overline{T}|$，称 $|\overline{T}|$ 为子式 $|T|$ 的余子式。其实 $|T|$ 与 $|\overline{T}|$ 是互为余子式的。

设A为n阶方阵。任取A的（i，j）位置处的元素a_{ij}。于是一阶子式$|a_{ij}|=a_{ij}$的余子式是$n-1$阶行列式，记作$|A_{ij}|$。我们把

$$(-1)^{i+j}|A_{ij}|$$

叫做元素a_{ij}的**代数余子式**。从而由n^2个元素a_{ij}的各个代数余子式（共有n^2个）确定一个n阶方阵

$$A^*=(b_{ij}),\ b_{ij}=(-1)^{j+i}|A_{ji}|.$$

称这样确定的n阶方阵A^*为A的**伴随矩阵**。矩阵A的伴随矩阵A^*的一个值得注意的显著特点就是A^*的各行元素依次是矩阵A的各列元素的代数余子式。

定理 6 设R为有恒等元素的交换环，$A\in M_n(R)$。则有

（1）
$$|A|=(-1)^{1+j}a_{1j}|A_{1j}|+(-1)^{2+j}a_{2j}|A_{2j}|+\cdots+(-1)^{n+j}a_{nj}|A_{nj}|,$$
$$|A|=(-1)^{i+1}a_{i1}|A_{i1}|+(-1)^{i+2}a_{i2}|A_{i2}|+\cdots+(-)^{i+n}a_{in}|A_{in}|$$

其中$1\leqslant j\leqslant n$，$1\leqslant i\leqslant n$。

（2）
$$(-1)^{1+j}a_{1i}|A_{1j}|+(-1)^{2+j}a_{2i}|A_{2j}|+\cdots+(-1)^{n+j}a_{ni}|A_{nj}|=0,$$
$$(-1)^{i+1}a_{j1}|A_{i1}|+(-1)^{i+2}a_{j2}|A_{i2}|+\cdots+(-1)^{i+n}a_{jn}|A_{in}|=0,$$

其中$1\leqslant i$，$j\leqslant n$，但$i\neq j$。

证 首先，我们根据行列式的定义来证明（1）的第一个等式成立，即行列式$|A|$的按列展开公式。为此，我们考察$M_n(R)$到R的映射：

$$\varphi: A=(a_{ij})\longmapsto\sum_{s=1}^{n}(-1)^{s+j}a_{sj}|A_{sj}|$$

我们去证这个映射φ就是$M_n(R)$上的行列式函数。

先指出映射φ是交错的。令α_1，α_2，…，α_n依次是A的n个

行。如果有$\alpha_k=\alpha_t$，$1\leqslant k<t\leqslant n$。那么可有，当$s\neq k$，$s\neq t$时，$n-1$阶行列式

$$|A_{sj}|=O。$$

这是因为，此时$|A_{sj}|$中有两个行是相同的缘故。当$s=k$时，行列式$|A_{kj}|$可以由行列式$|A_{tj}|$依次把第k行与第$k+1$，…，第$t-1$各行相交换而得到。这个过程一共做了$t-(k+1)=t-k-1$次行的交换，从而由定理5，可得

$$|A_{kj}|=(-1)^{t-k-1}|A_{tj}|$$

由此便得

$$\varphi(A)=(-1)^{k+j}a_{kj}|A_{kj}|+(-1)^{t+j}a_{tj}|A_{tj}|$$

把$|A_{kj}|$用$|A_{tj}|$的表示式来代替，以及$a_{kj}=a_{tj}$，则有

$$\varphi(A)=a_{kj}\ ((-1)^{t+j-1}|A_{tj}|+(-1)^{t+j}|A_{tj}|)$$

$$=a_{kj}\cdot O=O。$$

这就证明了φ是交错的。

其次证明φ是n重线性的。如果A的第r行为

$$\alpha_r=k\alpha_r'+l\alpha_r''。$$

用$B=(b_{ij})$表示各行依次为

$$\alpha_1,\ \cdots,\ \alpha_{r-1},\ \alpha_r',\ \alpha_{r+1},\ \cdots,\ \alpha_n$$

的n阶方阵。

用$C=(c_{ij})$表示各行依次为

$$\alpha_1,\ \cdots,\ \alpha_{r-1},\ \alpha_r'',\ \alpha_{r+1},\ \cdots,\ \alpha_n$$

的n阶方阵。往证：$\varphi(A)=k\varphi(B)+l\varphi(C)$

为此，我们具体观察A的第j列元素

$$a_{ij}:a_{1j},\ a_{2j},\ \cdots,\ a_{rj},\ \cdots,\ a_{nj}$$

的各个余子式$|A_{ij}|$，$i=1,\ 2,\ \cdots,\ n$。

当$i=r$时，则有

$$|A_{rj}|=|B_{rj}|=|C_{rj}|,$$

即此时元素a_{rj}、b_{rj}、c_{rj}在A、B、C中的余子式是一致的。从而，由于$a_{rj}=kb_{rj}+lc_{rj}$，则有

$$a_{rj}|A_{rj}| = (kb_{rj}+lc_{rj})|A_{rj}|$$
$$= kb_{rj}|B_{rj}| + lc_{rj}|C_{rj}|.$$

当$i\neq r$时，显然有 $a_{ij}=b_{ij}=c_{ij}$.并且，a_{ij}的余子式$|A_{ij}|$，作为$n-1$阶行列式，关于它的每一行都是线性的。因此，可得

$$|A_{ij}| = k|B_{ij}| + l|C_{ij}|$$

从而便得

$$a_{ij}|A_{ij}| = a_{ij}(k|B_{ij}| + l|C_{ij}|)$$
$$= kb_{ij}|B_{ij}| + lc_{ij}|C_{ij}|.$$

这样就有

$$\varphi(A) = k\varphi(B) + l\varphi(C),$$

即 φ 是 n 重线性的。

最后，当 $A=I_n$ 时，明显可知 $\varphi(I_n)=1_R$。总括以上所述，证明了 φ 是行列式函数，即（1）中的第一个等式对任意一个 j $(1\leqslant j\leqslant n)$ 都成立。

利用转置矩阵的行列式不变，可知（1）的第二个等式对任意的 $i(1\leqslant i\leqslant n)$ 都成立。

下面证明（2）中的两个等式成立。

已知 $A=(a_{ij})$，行向量依次为 $\alpha_1, \alpha_2, \cdots, \alpha_n$。令$D=(d_{ij})$，它的行向量依次为 $\alpha_1,\cdots,\alpha_{i-1}, \alpha_j, \alpha_{i+1}, \cdots, \alpha_j, \cdots, \alpha_n$。于是，对每一个$k$，均有

$$d_{ik} = a_{jk} = d_{jk}$$

由于行列式的交错性质，显然有 $|D|=O$。于是

$$(-1)^{i+1}a_{j1}|A_{i1}| + (-1)^{i+2}a_{j2}|A_{i2}| + \cdots + (-1)^{i+n}a_{jn}|A_{in}|$$
$$= (-1)^{i+1}d_{i1}|D_{i1}| + (-1)^{i+2}d_{i2}|D_{i2}| + \cdots + (-1)^{i+n}d_{in}|D_{in}|$$
$$= |D| = O$$

这就证明了（2）中的第二个等式成立。利用转置矩阵的行列式不变，可知（2）的第一个等式也成立。▌

推论 1. $A^*A=|A|I_n=AA^*$

2. A是可逆矩阵$\Longleftrightarrow$ $|A|$是环R中的可逆元素.

3. A是可逆矩阵$\Longleftrightarrow$存在矩阵B，使得$AB=I_n$$\Longleftrightarrow$存在矩阵$C$，使得$CA=I_n$.

事实上推论1是定理6的矩阵表现形式.

推论2的必要性已如定理4之（5）所述. 而当$|A|$是环R的可逆元素时，由推论1可知矩阵$|A|^{-1}A^*$就是A的逆阵，即

$$A^{-1}=|A|^{-1}A^*$$

推论3是推论2的推论. ▌

定理6（1）中的两个式子通常叫做行列式的按列(按行)展开式. 下面讨论行列式展开式的一般形式，即熟知的拉普拉斯定理，它是定理6（1）的推广.

设$A=(a_{ij})$是环R（有恒等元素、交换）上的n阶方阵. 所谓A的行列式$|A|=a\in R$，它是由行列式函数d给"自变量"A取定的"函数值"：

$$d(A)=a$$

按定义，行列式函数d是以$M_n(R)$为定义域，以R为值域的一个函数，满足下面的三个条件：

（1）关于每一个行d都是线性的.

（2）关于行d是交错的.

（3）单位阵I_n的函数值等于R的恒等元素：

$$d(I_n)=1_R.$$

按定理3，在$M_n(R)$上存在唯一的行列式函数d.

按定理4，$M_n(R)$上唯一存在的那个行列式函数d可以"构造性"的表达成一个代数和：

$$d(A)=\sum_{\sigma\in S_n} sgn\sigma\, a_{1\sigma(1)}a_{2\sigma(2)}\cdots a_{n\sigma(n)},$$

或者

$$d(A)=\sum_{j_1j_2\cdots j_n\in S_n}(-1)^{\tau(j_1j_2\cdots j_n)}a_{1j_1}a_{2j_2}\cdots a_{nj_n}.$$

我们把这个代数和叫做行列式函数 d 的表达式，也具体地叫做 n 阶方阵 A 的行列式 $|A|$ 的表达式。对于表达式中的乘积：

$$a_{1j_1}a_{2j_2}\cdots a_{nj_n}.$$

叫做行列式 $d(A)$ 的一个项，同时相应地把符号

$$(-1)^{\tau(j_1j_2\cdots j_n)}$$

叫做项 $a_{1j_1}a_{2j_2}\cdots a_{nj_n}$ 的符号。这样，明显可见，行列式 $d(A)$ 的表达式有以下特征：

（1）n 阶方阵 A 的行列式 $d(A)$ 的表达式是由 $n!$ 个项构成的代数和。

（2）每一个项 $a_{1j_1}a_{2j_2}\cdots a_{nj_n}$ 均由阵 A 的 n 个元素相乘而成；并且这 n 个元素

$$a_{1j_1},\ a_{2j_2},\ \cdots,\ a_{nj_n},$$

对阵 A 来说，既不在相同的行上也不在相同的列上。

（3）项 $a_{1j_1}a_{2j_2}\cdots a_{nj_n}$ 的符号由列下标 j_1，j_2，…，j_n 构成的排列

$$j_1j_2\cdots j_n$$

的奇偶性来确定。当排列

$$j_1j_2\cdots j_n$$

是偶排列时，项 $a_{1j_1}a_{2j_2}\cdots a_{nj_n}$ 前边的符号取正号；当排列

$$j_1j_1\cdots j_n$$

是奇排列时，项 $a_{1j_1}a_{2j_2}\cdots a_{nj_n}$ 前边的符号取负号。即

$$(-1)^{\tau(j_1j_2\cdots j_n)}=\begin{cases}+, & j_1j_2\cdots j_n\text{ 为偶排列；}\\ -, & j_1j_2\cdots j_n\text{ 为奇排列。}\end{cases}$$

n 阶方阵 A 的 k 阶子式 $|T|$ 也叫做是行列式 $|A|$ 的 k 阶子式。令 $|\overline{T}|$ 是子式 $|T|$ 的余子式。如果子式 $|T|$ 的各行依次是 A 的第 i_1 行，第 i_2 行，…，第 i_k 行；$|T|$ 的各列依次是 A 的第 j_1 列，第 j_2 列，…，

第j_k列，那么称

$$(-1)^{i_1+i_2+\cdots+i_k+j_1+j_2+\cdots+j_k}|\overline{T}|$$

为子式$|T|$的代数余子式。

定理 7（拉普拉斯定理）设在n阶方阵A中任意取定了k($1\leqslant k\leqslant n-1$)个行。由这$k$行元素所组成的一切$k$阶子式与它们的代数余子式的乘积的和等于$A$的行列式$|A|$。

证 设在A中取定k行后得到的子式为：

$$|T_1|, |T_2|, \cdots, |T_u|;$$

它们的代数余子式依次为

$$|S_1|, |S_2|, \cdots, |S_u|$$

这样，定理 7 要求证明

$$|A|=|T_1|\cdot|S_1|+|T_2|\cdot|S_2|+\cdots+|T_u|\cdot|S_u|.$$

我们分两步来证明上述这个等式成立。首先指出乘积

$$|T_r|\cdot|S_r|, \qquad r=1, 2, \cdots, u$$

中的每一项都是行列式$|A|$的表达式中的一项，而且符号也一致。

我们首先讨论T_r位于A的左上方的情形：

$$|A|=\begin{vmatrix} a_{11} & a_{12} & \cdots & a_{1k} & a_{1\,k+1} & \cdots & a_{1n} \\ \cdot & T_r & \cdots & \cdot & \cdot & & \cdots \\ a_{k1} & a_{k2} & \cdots & a_{kk} & a_{k\,k+1} & \cdots & a_{kn} \\ a_{k+1\,1} & a_{k+1\,2} & \cdots & a_{k+1\,k} & a_{k+1\,k+1} & \cdots & a_{k+1\,n} \\ \cdot & \cdot & \cdots & \cdot & \cdot & \overline{T}_r & \cdot \\ a_{n1} & a_{n2} & \cdots & a_{nk} & a_{n\,k+1} & \cdots & a_{nn} \end{vmatrix}$$

此时子式$|T_r|$的代数余子式为

$$|S_r|=(-1)^{(1+2+\cdots+k)+(1+2+\cdots+k)}|\overline{T}_r|$$

$$=|\overline{T}_r|$$

k阶行列式$|T_r|$的每一项都可写作

$$a_{1i_1}a_{2i_2}\cdots a_{ki_k},$$

其中$i_1i_2\cdots i_k$是1, 2, $\cdots$, k的一个排列。从而这一项前面的

符号为

$$(-1)^{\tau(i_1 i_2 \cdots i_k)}$$

$(n-k)$ 阶行列式 $|\overline{T}_r|$ 的每一项都可写作

$$a_{k+1\ j_{k+1}} a_{k+2\ j_{k+2}} \cdots a_{n j_n},$$

其中 $j_{k+1} j_{k+2} \cdots j_n$ 是 $k+1$, $k+2$, …, n 的一个排列. 从而这一项前面的符号应为

$$(-1)^{\tau(j'_{k+1} j'_{k+2} \cdots j'_n)},$$

其中 $j'_s = j_s - k$, $s = k+1$, $k+2$, …, n.

于是乘积 $|T_r| \cdot |S_r| = |T_r| \cdot |\overline{T}_r|$ 展开之后的每一项都有以下形式:

$$a_{1 i_1} a_{2 i_2} \cdots a_{k i_k} a_{k+1\ j_{k+1}} a_{k+2\ j_{k+2}} \cdots a_{n j_n},$$

它前面的符号为

$$(-1)^{\tau(i_1 i_2 \cdots i_k)} \ (-1)^{\tau(j'_{k+1} j'_{k+2} \cdots j'_n)}$$

$$= (-1)^{\tau(i_1 i_2 \cdots i_k) + \tau(j'_{k+1} j'_{k+2} \cdots j'_n)}$$

$$= (-1)^{\tau(i_1 i_2 \cdots i_k j_{k+1} j_{k+2} \cdots j_n)}$$

因此, 乘积 $|T_r| \cdot |S_r|$ 的项都是行列式 $|A|$ 的表达式中的项, 并且符号也一致.

其次, 对于一般的情形, 即 T_r 不是恰好位于 $|A|$ 的左上方. 我们可以通过交换行列式 $|A|$ 的行、列的办法, 使其归结成为上述的特殊情形. 从而, 根据定理 5 之 (1) 同样得到: $|T_r| \cdot |S_r|$ 的项都是行列式 $|A|$ 的表达式中的项, 并且符号也一致.

第二步我们来考察各个乘积 $|T_r| \cdot |S_r|$ 的项数.

首先, $|T_r|$ 共有 $k!$ 项; $|S_r|$ 共有 $(n-k)!$ 项. 因此, 乘积 $|T_r| \cdot |S_r|$ 共有 $k!(n-k)!$ 个项. 并且显然是行列式 $|A|$ 的表达式中的 $k!(n-k)!$ 个不同的项.

其次, 任二不同的乘积 $|T_r| \cdot |S_r|$ 与 $|T_l| \cdot |S_l|$, $r \neq l$, 它们的项必为行列式 $|A|$ 的表达式中不同的项.

再次, 乘积 $|T_r| \cdot |S_r|$ 的个数

$$u = C_n^k = \frac{n!}{k!(n-k)!}$$

这样，这 u 个乘积总共的项数为

$$u \cdot k!(n-k)! = n!$$

总括以上所述，定理 7 ，即拉普拉斯定理被证明了。∎

下面介绍本节的最后一个问题，即矩阵的相抵关系以及主理想环上矩阵在相抵关系之下的标准形。

设 R为有恒等元素的交换环。

在前面我们已经提到过两个 n 阶方阵相似的概念。令 A 与B 是环R上的两个 n 阶方阵。如果存在R上的 n 阶可逆矩阵P，使得

$$B = PAP^{-1}$$

则称 A与B 是相似的，简称 A与B **相似**。

不难指出，相似关系是 n 阶方阵的集合 $M_n(R)$ 上的一个等价关系。即相似关系具有以下三条性质：

（1）反身性：A与A相似。

（2）对称性：若 A与B 相似则 B与A 相似。

（3）传递性：若 A与B 相似且 B与C相似则A与C相似。

其中 A，B，C为 $M_n(R)$ 中的任意元素。

这样，相似关系使$M_n(R)$ 的元素划分成类：

A 与 B 分在同一类$\Longleftrightarrow$$A$与$B$相似。

把 $M_n(R)$ 的元素划分成相似类，对高等代数中的线性空间与线性变换理论的作用及意义是明确的、重要的（这时 R是数域）。目前对一般情况来说，$M_n(R)$ 的相似分类在模的理论中同样有非常突出的作用。

现在我们来指出矩阵之间另外一种更为一般的关系——**相抵关系**。

设 A与B 是任意两个 $m\times n$矩阵（不必是$m=n$）。如果存在 m 阶可逆矩阵P和n阶可逆矩阵Q，使得

$$B = PAQ$$

则称A与B是相抵的，简称A与B相抵。

不难指出，相抵关系是一切$m\times n$矩阵的集合$M_{m\times n}(R)$上的一个等价关系，即相抵关系也具有以下三条性质：

（1）反身性：A与A相抵。

（2）对称性：若A与B相抵则B与A相抵。

（3）传递性：若A与B相抵且B与C相抵则A与C相抵。

其中A，B，C为$M_{m\times n}(R)$中的任意元素。

这样，相抵关系使$M_{m\times n}(R)$的元素划分成类：

A与B分在同一类$\Longleftrightarrow A$与B相抵。

把$M_{m\times n}(R)$的元素按相抵关系划分成类的重要作用和意义在高等代数中已经得到相当明显、突出和充分的体现。同样地，在模的理论中矩阵的相抵关系与相抵类也扮演着重要的角色。

矩阵的相抵分类与相似分类在线性代数的理论中之所以具有这般重要的作用和意义，关键在于，在相应的分类之下使得每一个类中均存在着唯一的一个所谓的“标准元素”，它具有简单、典型和规范的特性。关于相似分类的标准形问题放在后面去讨论。现在我们考虑主理想环R上$m\times n$矩阵相抵分类的标准形问题。

首先，象在高等代数中讨论矩阵的相抵标准形一样，引用初等矩阵和初等变换的概念是方便的。我们把以下三种形式的方阵统称为**初等矩阵**：

Ⅰ．消法矩阵

$$T_{ij}(b)=\begin{pmatrix}1 & & & & \\ & \ddots & & & \\ & & 1 & \cdots & b \\ & & & \ddots & \vdots \\ & & & & 1 \\ & & & & & \ddots \\ & & & & & & 1\end{pmatrix}$$

其中$b\in R$，在$T_{ij}(b)$的$(i,\ j)$位置，$i\neq j$。

Ⅱ. 倍法矩阵

$$D_i(u)=\begin{pmatrix}1&&&&&&\\&\ddots&&&&0&\\&&1&&&&\\&&&u&&&\\&&&&1&&\\&0&&&&\ddots&\\&&&&&&1\end{pmatrix}$$

其中 $u\in R$，是可逆元素。

Ⅲ. 换法矩阵

$$P_{ij}=\begin{pmatrix}1&&&&\\&\ddots&&&\\&&\begin{matrix}0&\cdots&1\\\vdots&\ddots&\vdots\\1&\cdots&0\end{matrix}&&\\&&&\ddots&\\&&&&1\end{pmatrix}.$$

这三种类型的初等矩阵与高等代数中的初等矩阵是完全一致的。值得注意的只有一点，即在倍法矩阵$D_i(u)$中，元素u不是一般的非零元素而是环 R中的可逆元素。

不难验算

$$T_{ij}(b)T_{ij}(-b)=I=T_{ij}(-b)T_{ij}(b);$$

$$D_i(u)D_i(u^{-1})=I=D_i(u^{-1})D_i(u);$$

$$P_{ij}^2=I,$$

其中 I 为单位方阵。这表明初等矩阵均为可逆矩阵，并且它们的逆阵也是同一类型的初等矩阵。

再有，对任一$m\times n$矩阵 A，用一个$m(n)$ 阶的初等矩阵从左（右）边去乘 A将得到怎样的一个矩阵 B，是众所周知的。我们就不赘述了。相应地，叫做对 A 的行（列）做一次初等变换，例如，

$$T_{ij}(b)A=B$$

时，就说对A的行做一次消法变换$T_{ij}(b)$得到B。再如

$$AD_i(u)=C$$

时，就说对A的列做一次倍法变换$D_i(u)$得到C。显然，对A做初等变换得到的阵都是与A相抵的。

现在就来证明重要的

定理 8 设R是主理想环。R上任一$m\times n$矩阵A必相抵于如下的对角形阵：

$$diag\{d_1,d_2,\cdots,d_r,0,\cdots,0\}=\begin{pmatrix} d_1 & & & & & \\ & d_2 & & & & \\ & & \ddots & & & \\ & & & d_r & & \\ & & & & 0 & \\ & & & & & \ddots \\ & & & & & & 0 \end{pmatrix}$$

其中$d_i\neq 0$且$d_1|d_2|\cdots|d_r$，$i=1,2,\cdots,r$。

显然，这个定理 8是高等代数中用初等变换简化λ——矩阵为标准形相应定理的一般化。证明的思路与方法二者完全类似。称定理 8 中的对角形阵为法对角形。这样，定理 8 的意思是，对于主理想环R上的$m\times n$矩阵来说，每一个相抵类中都只少有一个相当简单、典型和规范的矩阵——法对角形。换个说法也就是主理想环R上的每一个$m\times n$矩阵A都和某一个法对角形阵相抵。

定理 8 的证明。我们分两种情形来考虑：

1）R是特殊的主理想环——欧氏环。这时R很象域F上的多项式环$F[\lambda]$，R中每一个非零元素a均有一个象征性的"次数"$\delta(a)$——非负整数，并且能象多项式一样做带余除法。正因为这样，此时定理 8 的证明与大家相当熟悉的高等代数中相应定理的证明几乎完全一样。从而不会感到有什么困难。

具体做法如下：若$A=0$，这时没什么要说的，可以认为定理 8 的结论自然是对的。如果$A\neq 0$，那么必有A的元素$a_{ij}\neq 0$，且a_{ij}的"次数"$\delta(a_{ij})\leqslant A$中其它非零元素的"次数"。利用

换法变换，可将这个 a_{ij} 移到第一行、第一列的位置。于是，当 $A\neq 0$ 时，总可以假定 $a_{11}\neq 0$，且"次数" $\delta(a_{11})$ 小于或等于 A 中其它非零元素的"次数"。这时，如果第一行的其它元素都能被 a_{11} 整除，那么利用消法变换可把第一行除 a_{11} 以外的元素都化简为 0。如果第一行有元素 a_{1k} 不能被 a_{11} 整除，于是按欧氏环 R 中的带余除法，则有

$$a_{1k}=a_{11}g_k+r_{1k},\quad \delta(r_{1k})<\delta(a_{11}),$$

这样，利用消法变换把 (1, k) 位置的元素 a_{1k} 化为 r_{1k}。接着再利用换法变换把 r_{1k} 换到第一行第一列的位置。

由于欧氏环 R 中非零元素 a 的"次数"$\delta(a)$ 是非负整数，它不可能无限制的降低下去。因而，我们重复上述的办法，总可以把第一行除了第一列位置的元素外，其它元素都化简为 0。对 A 施行上述变换的每一步骤所得到的新阵与原矩阵 A 都是相抵的。

用类似的办法化简第一列，同样可把第一列除第一行位置的元素外，其它元素都化简为 0。从而得到与 A 相抵的矩阵：

$$B=\begin{pmatrix} b_{11} & 0 & \cdots & 0 \\ 0 & b_{22} & \cdots & b_{2n} \\ \cdot & \cdot & \cdots & \cdot \\ 0 & b_{m2} & \cdots & b_{mn} \end{pmatrix}$$

把以上办法再用于矩阵

$$B_0=\begin{pmatrix} b_{22} & \cdots & b_{2n} \\ \cdot & \cdots & \cdot \\ b_{m2} & \cdots & b_{mn} \end{pmatrix}$$

这时所需要做的初等变换并不影响矩阵 B 的第一行与第一列。于是，可以得到与 B，从而也就与 A，相 抵的具有以下形状的矩阵：

$$C=\begin{pmatrix} b_{11} & 0 & 0 & \cdots & 0 \\ 0 & c_{22} & 0 & \cdots & 0 \\ 0 & 0 & c_{33} & \cdots & c_{3n} \\ \cdot & \cdot & \cdot & \cdots & \cdot \\ 0 & 0 & c_{m3} & \cdots & c_{mn} \end{pmatrix}$$

这样继续做下去，经过有限次的初等变换，最后得出与A相抵的对角形阵：

$$C_1=\begin{pmatrix} c_1 & & & & & \\ & c_2 & & & 0 & \\ & & \ddots & & & \\ & & & c_r & & \\ & & & & 0 & \\ & & & & & \ddots \\ & 0 & & & & 0 \end{pmatrix},$$

其中 $c_i \neq 0$，$i=1, 2, \cdots, r$。

在此基础上，我们希望通过初等变换，把对角形阵C_1进一步化简，使之满足

$$c_1 \backslash c_2 \backslash c_3 \backslash \cdots \backslash c_r,$$

即对角线上的元素自上而下的依次能整除。

如果尚且c_i不能整除c_j，$i<j$。那么可令

$$c_j=c_iq_j+r_j,\ \delta(r_j)<\delta(c_i).$$

于是，可得相抵于C_1（从而也相抵于A）的矩阵

$$C_2=\begin{pmatrix} c_1 & & & & & & \\ & \ddots & & & & & \\ & & c_i \cdots c_j & & & & \\ & & \ddots \ \vdots & & & & \\ & & & c_j & & & \\ & & & & \ddots & & \\ & & & & & c_r & \\ & & & & & & 0 \\ & & & & & & & \ddots \\ & & & & & & & & 0 \end{pmatrix},$$

用若干次适当的初等变换，又可把C_2化简成

$$C_3=\begin{pmatrix} c_1' & & & & & & \\ & \ddots & & & & & \\ & & c_i' & & & & \\ & & & \ddots & & & \\ & & & & c_j' & & \\ & & & & & \ddots & \\ & & & & & & c_r' \\ & & & & & & & 0 \\ & & & & & & & & \ddots \\ & & & & & & & & & 0 \end{pmatrix}$$

以上过程表明，通过有限次适当的初等变换之后，一定能够得到一个对角形阵：

$$\begin{pmatrix} d_1 & & & & & & \\ & d_2 & & & & & \\ & & \ddots & & & & \\ & & & d_r & & & \\ & & & & 0 & & \\ & & & & & \ddots & \\ & & & & & & 0 \end{pmatrix},$$

且满足 $d_1 \diagdown d_2 \diagdown \cdots \diagdown d_r$.

到此已经证明了，当 R 是特殊的主理想环——欧氏环时，R 上的 $m\times n$ 矩阵 A 必相抵于一个法对角形阵：

$$diag\{d_1,\ d_2,\ \cdots,\ d_r,\ 0,\ \cdots,\ 0\},\ d_1 \diagdown d_2 \diagdown \cdots \diagdown d_r.$$

2）R 是一般的主理想环．现在有了1）的推理过程，对这一般情形也就容易做到心中有数了．这时我们使用元素的“长度”来代替上面的“次数”．

把主理想环 R 中的非零元素 a 分解为不可约元素的乘积，根据因子分解唯一性定理，在 a 的这样的分解式中不可约因子的个数是由a所唯一决定的．把这样一个确定的正整数叫做元素a的“长度”，并记作 $l(a)$．当 a 是主理想环 R 中的可逆元素时，规定 a 的“长度”为 $l(a)=0$．

于是，同1）的情形一样，我们可以假定非零矩阵 A中元素

$a_{11}\neq 0$，而且其长度 $l(a_{11})$ 小于或等于 A 中其它非零元素的长度。如果 A 中第一行除a_{11}外其余元素都能被 a_{11}整除，那么用消法变换可将这些元素化为 0 .否则，假如有 a_{1k}不能被a_{11}整除。令

$$a=a_{11},\ b=a_{1k}\ 且\ (a,\ b)=d,$$

即 a 与 b 的最大公因子为 d。这样，存在元素 $x,\ y\in R$，使得

$$ax+by=d.$$

于是，对于 $a,\ d$ 与 $b,\ d$ 存在元素 $t,\ s\in R$，使得

$$dt=-a,\ ds=b.$$

从而 $-dtx+dsy=d$，故而 $-tx+sy=1$. 由此，可有矩阵的关系式：

$$\begin{pmatrix} -t & s \\ y & -x \end{pmatrix}\begin{pmatrix} x & s \\ y & t \end{pmatrix}=\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

这说明矩阵

$$\begin{pmatrix} -t & s \\ y & -x \end{pmatrix},\ \begin{pmatrix} x & s \\ y & t \end{pmatrix}$$

都是可逆的。因此矩阵

$$U=\begin{pmatrix} x & 0 & \cdots & 0 & s & 0 & \cdots & 0 \\ 0 & 1 & \cdots & 0 & 0 & 0 & \cdots & 0 \\ \cdot & \cdot & \cdots & \cdot & \cdot & \cdot & \cdots & \cdot \\ 0 & 0 & \cdots & 1 & 0 & 0 & \cdots & 0 \\ y & 0 & \cdots & 0 & t & 0 & \cdots & 0 \\ & & & & & 1 & \cdots & 0 \\ & & & & & & \ddots & \vdots \\ & & & & & & & 1 \end{pmatrix},$$

（第 k 列为 (k) 列，第 k 行为 (k) 行）

也是可逆的。用这个矩阵U从右边去乘矩阵A得AU，其第一行的元素为

$$(d,\ a_{12},\ \cdots,\ a_{1k-1},\ 0,\ a_{1k+1},\ \cdots,a_{1n}),$$

其中 $l(d)<l(a_{11})$。

如果这时 d 能整除任何的 a_{1j} $(j=2,\ \cdots,\ k-1,k+1,\cdots,n)$，那么用消法变换可将 AU 的第一行除了第一列的元素之外都化简成 0。否则，再用类似于U 的矩阵去右乘 AU，将可得到一个左上角元素的长度小于 $l(d)$ 的相抵于 AU 的矩阵。由于主理想环中非零元素的长度是一个非负整数，从而它不可能无限制的减少下去。因此，经过有限的步骤，得到一个相抵于 A的矩阵，它的第一行元素除了第一列的一个元素之外，其它元素均已为 0。

同样的办法用于第一列，将能进一步得到一个相抵于 A的矩阵，它的第一列除了第一行的一个元素之外均化简为 0。这样，A 就相抵于以下形式的矩阵：

$$\begin{pmatrix} d & 0 & \cdots & 0 \\ 0 & b_{22} & \cdots & b_{2n} \\ \cdot & \cdot & \cdots & \cdot \\ 0 & b_{m2} & \cdots & b_{mn} \end{pmatrix}.$$

接下去把上述的论证用于阶数降低了的矩阵

$$\begin{pmatrix} b_{22} & \cdots & b_{2n} \\ \cdot & \cdots & \cdot \\ b_{m2} & \cdots & b_{mn} \end{pmatrix}$$

这样，最终就能得到相抵于 A的法对角形阵。到此，定理 8 被完全证明了。▌

上述的定理 8 只是肯定了主理想环 R上的$m\times n$矩阵的每一个相抵类中都存在一个非常特殊的矩阵——法对角形阵。进一步的问题是这样的法对角形阵是否是唯一的。为了解决这个唯一性问题，我们需要矩阵的秩数与行列式因子这样两个概念。

设A为主理想环上的一个$m\times n$矩阵。如果在 A的各阶子式中

有不等于零的 r 阶子式，但是阶数高于 r 的子式都等于零，则称矩阵 A 的秩数等于 r，简称 A 的秩为 r，记作

$$\mathrm{rank} A = r$$

特别地，当 $A=0$ 时，规定 A 的秩为 0。

如果A的秩为r，且$r>0$，那么对于任意一个k：$1\leqslant k\leqslant r$，矩阵 A 必有不等于零的 k 阶子式。从而，对于A的一切 k阶子式来说，存在着不等于零的最高公因子，记作 Δ_k，并叫做是 A的 k 阶**行列式因子**。这样，秩为 r 的矩阵 A恰有 r 个行列式因子：

$$\Delta_1,\ \Delta_2,\ \cdots,\ \Delta_r,$$

其中 Δ_k 为矩阵 A 的 k 阶行列式因子，$k=1,\ 2,\ \cdots,\ r$。

定理 9 设 R 为主理想环，A与B为 R 上的两个$m\times n$矩阵。则有

（1）令 A 的秩为 r，行列式因子为

$$\Delta_1,\ \Delta_2,\ \cdots,\ \Delta_r;$$

B 的秩为 s，行列式因子为

$$\Delta_1',\ \Delta_2',\ \cdots,\ \Delta_s'$$

如果 A 与 B 相抵，那么 $r=s$，并且

$$\Delta_1'=c_1\Delta_1,\quad \Delta_2'=c_2\Delta_2,\quad \cdots,\quad \Delta_r'=c_r\Delta_r,$$

其中 $c_1,\ c_2,\ \cdots,\ c_r$ 是环R中的可逆元素。

（2）如果 A是法对角形阵：

$$A=diag\{d_1,\ d_2,\ \cdots,\ d_r,\ 0,\ \cdots,\ 0\},$$

并且 $d_1\diagdown d_2\diagdown\cdots\diagdown d_r$。那么 A 的秩等于 r，行列式因子为

$$\Delta_1=d_1,\ \Delta_2=d_1d_2,\ \cdots,\ \Delta_r=d_1d_2\cdots d_r.$$

（3）如果 A 与 B 都是 R 上的 $m\times n$阶法对角形阵并且 A与 B 是相抵的：

$$A=diag\{d_1,\ d_2,\ \cdots,\ d_r,\ 0,\ \cdots,\ 0\},$$

其中 $d_1\diagdown d_2\diagdown\cdots\diagdown d_r$；

$$B=diag\{d_1',d_2',\cdots,d_s',0,\cdots,0\},$$

其中 $d_1'\diagdown d_2'\diagdown\cdots\diagdown d_s'$，那么 $r=s$，并且

$$d_1' = u_1 d_1,\ d_2' = u_2 d_2,\ \cdots,\ d_r' = u_r d_r,$$

其中 $u_1, u_2, \cdots, u_r$ 为环 R中的可逆元素.

证 首先证明（1）成立. 为此我们分两种特殊情形来考虑. 先看 $B = PA$的情形，其中 P是任意一个m阶可逆方阵. 这时，我们不难注意到，矩阵 B的每一行都是矩阵A的 m个行的线性组合. 因此，B的任意一个k阶子式均可表成 A的一些k阶子式的线性组合. 从而可以断定：

1）$rankB \leqslant rankA$，即$s \leqslant r$；

2）A的k阶行列式因子 Δ_k整除B的k阶行列式因子 Δ_k'，即 $\Delta_k \diagdown \Delta_k'$.

由对称性：即$B = PA \Longrightarrow A = P^{-1}B$，即得：

$r \leqslant s$，从而 $s = r$；

$\Delta_k' \diagdown \Delta_k$，从而 $\Delta_k' = c_k \Delta_k$，c_k为环 R中的可逆元素，$k = 1, 2, \cdots, r$.

再看 $B = AQ$的情形，其中 Q是任意一个n阶可逆方阵. 这时，我们不难注意到，矩阵 B的每一列都是矩阵 A的 n 个列的线性组合. 因此，同样是根据行列式的性质，便可得到：

$s = r$；

$\Delta_k' = c_k \Delta_k$，c_k为环 R 中的可逆元素，$k = 1, 2, \cdots, r$.

把以上的两种特殊情形结合起来，即得：两个相抵的矩阵 A与 B必有相同的秩数以及同阶的行列式因子只差 R中的一个可逆元素的倍数，亦即（1）成立.

其次说明（2）成立. 令 A为法对角形阵：

$$A = diag\{d_1, d_2, \cdots, d_r, 0, \cdots, 0\},$$

其中 $d_i \diagdown d_{i+1} \diagdown$，$i = 1, 2, \cdots, r-1$，且 $d_1, d_2, \cdots, d_r$均不为0.

这时，不难说明，如果 A的一个k阶子式所包含的 k个行与k个列的序号不完全一致时，那么这个k阶子式等于0. 因此，A的非零的k阶子式只有以下的形式：

$$\begin{vmatrix} d_{i_1} & & & \\ & d_{i_2} & & \\ & & \ddots & \\ & & & d_{i_k} \end{vmatrix} = d_{i_1} d_{i_2} \cdots d_{i_k}$$

从而便可得到：

1）$rankA = r$；

2）$\Delta_1 = d_1$，$\Delta_2 = d_1 d_2$，…，$\Delta_r = d_1 d_2 \cdots d_r$。

即（2）成立。

最后，证明（3）成立。设A与B是相抵的两个法对角形矩阵：

$$A = diag\{d_1, d_2, \cdots, d_r, 0, \cdots, 0\},$$

其中 d_1，d_2，…，d_r，均不为零，且 $d_1 \backslash d_2 \backslash \cdots \backslash d_r$；

$$B = diag\{d_1', d_2', \cdots, d_s', 0, \cdots, 0\}$$

其中，d_1'，d_2'，…，d_s' 均不为零，且 $d_1' \backslash d_2' \backslash \cdots \backslash d_s'$。

令 A与 B 的行列式因子分别为

$$\Delta_1, \Delta_2, \cdots, \Delta_r;$$

$$\Delta_1', \Delta_2', \cdots, \Delta_s'.$$

于是，由已经证明过的（1）与（2），可知：

1）$rankA = r$，$rankB = s$，且 $s = r$；

2）$\Delta_1 = d_1$，$\Delta_2 = d_1 d_2$，…，$\Delta_r = d_1 d_2 \cdots d_r$；

$\Delta_1' = d_1'$，$\Delta_2' = d_1' d_2'$，…，$\Delta_r' = d_1' d_2' \cdots d_r'$。

3）$\Delta_1' = c_1 \Delta_1$，$\Delta_2' = c_2 \Delta_2$，…，$\Delta_r' = c_r \Delta_r$，

其中 c_1，c_2，…，c_r 均为环 R 中的可逆元素。

这样，由 2），又可写成如下的关系式：

$$d_1 = \Delta_1,\ d_2 = \Delta_2 \Delta_1^{-1},\ \cdots,\ d_r = \Delta_r \Delta_{r-1}^{-1}$$

此处之 $\Delta_i \Delta_{i-1}^{-1}$表示等式 $\Delta_i = q_i \Delta_{i-1}$中的$q_i$；

$$d_1' = \Delta_1',\ d_2' = \Delta_2' \Delta_1'^{-1},\ \cdots,\ d_r' = \Delta_r' \Delta_{r-1}'^{-1},$$

此处之 $\Delta_i' \Delta_{i-1}'^{-1}$表示等式 $\Delta_i' = q_i' \Delta_{i-1}'$中的 q_i'。

于是，再由 3），便可得到：

$$d_1'=b_1d_1,\ d_2'=b_2d_2,\ \cdots,\ d'_r=b_rd_r,$$

其中 b_1，b_2，…，b_r 均为 R 中的可逆元素. 这样，又证明了（3）成立。到此定理 9 证明完了. ▌

定理 9 的重要意义在于它完全揭示了主理想环R上 $m\times n$矩阵在相抵分类之下的不变量. 由定理 9 之 3)，两个相抵的法对角形阵的差别只是对角线上的非零元素 d_1，d_2，…，d_r 相差环R中的一个适当的可逆元素. 对于同属于一个相抵类中的两个法对角形阵来说，这种差别是自然的，不可避免的. 这样，在不计较这种不可避免的差别的意义下，我们把主理想环 R上的法对角形阵叫做 R 上的**标准形矩阵**，同时把矩阵 A 所相抵的标准形阵

$$diag\{d_1,\ d_2,\ \cdots,\ d_r,\ \ 0,\ \cdots,\ \ 0\}$$

中的非零元素 d_1，d_2，…，d_r 叫做 A的**不变因子组**，而称d_i为A的第 i 个**不变因子**，$i=1,\ 2,\ \cdots,\ r$.

推论 在不计较可逆元素的倍数之意义下，主理想环 R上的 $m\times n$ 矩阵A都相抵于唯一的一个标准形；从而A有唯一的不变因子组. ▌

定理10 设A与B为主理想环R上的两个$m\times n$矩阵. 则有

A与 B 相抵$\Longleftrightarrow$$A$与$B$的标准形相同.

$\Longleftrightarrow$$A$与 B 的不变因子相同.

$\Longleftrightarrow$$A$与 B 的行列式因子相同.

证 必要性已如定理 9 所述. 利用行列式因子与不变因子之间的相互关系：

$$\Delta_1=d_1,\ \ \Delta_2=d_1d_2,\ \cdots,\ \ \Delta_r=d_1d_2\cdots d_r;$$

$$d_1=\Delta_1,\ d_2=\Delta_2\,\Delta_1^{-1},\ \cdots,\ d_r=\Delta_r\,\Delta_{r-1}^{-1},$$

便可证明定理10的另外一方面的结论. ▌

在不变因子的基础上，我们再给出初等因子的概念，这在后面的讨论问题时会用得到的.

设矩阵 A的标准形为

$$diag\{d_1,\ d_2,\ \cdots,\ d_r,\ 0,\cdots,0\},$$

在A的不变因子$d_1,\ d_2,\ \cdots,\ d_r$中，因为是依次能整除的，所以如果其中有可逆元素的话，一定是前边的某几个。这样可令

$$d_1,\ d_2,\ \cdots,\ d_{i-1}$$

都是可逆元素。而

$$d_i,\ d_{i+1},\ \cdots,\ d_r$$

都不是可逆元素。

于是，把$d_i,\ d_{i+1},\ \cdots,\ d_r$在主理想环$R$中写出它们的标准分解式：

$$d_i = p_1^{l_{i1}} p_2^{l_{i2}} \cdots p_t^{l_{it}},$$

$$d_{i+1} = p_1^{l_{i+1\,1}} p_2^{l_{i+1\,2}} \cdots p_t^{l_{i+1\,t}}.$$

$$\vdots$$

$$d_r = p_1^{l_{r1}} p_2^{l_{r2}} \cdots p_t^{l_{rt}}.$$

其中对任意的$k=1,\ 2,\ \cdots,\ t$，都有

$$0 \leqslant l_{ik} \leqslant l_{i+1\,k} \leqslant \cdots \leqslant l_{rk}.$$

我们把上述标准分解式中出现的指数不等于零的幂

$$p_k^{l_{jk}};\ j=i,\ i+1,\ \cdots,\ r,\ k=1,\ 2,\ \cdots,\ t,$$

叫做属于p_k的一个**初等因子**。属于各个p_k的一切初等因子叫做A的**初等因子组**。显然，A的初等因子组是由A的不变因子所唯一决定的。反过来，在事先给定了一组有限个不可约元素的幂之后，不难拼凑成有限个元素：

$$\overline{d_1},\ \overline{d_2},\ \cdots,\ \overline{d_S},$$

使得，$\overline{d_1} \diagdown \overline{d_2} \diagdown \cdots \diagdown \overline{d_S}$，并且$\overline{d_1}, \overline{d_2},\ \cdots,\ \overline{d_S}$的标准分解式中出现的一切指数不等于零的不可约元素的幂恰好就是当初给定的那一组不可约元素的幂。而且$\overline{d_1},\ \overline{d_2},\ \cdots,\ \overline{d_S}$是由给定的不可约元素的幂所唯一决定的。于是，在指定了秩数r的条件下，存在唯一的标准形矩阵A，以事先给定的一组不可约元素的幂为初等因子

组．换个说法，在指定了秩数的条件下，不变因子也是由初等因子唯一决定的．以上所述不变因子与初等因子之间的关系可以表达成如下的

定理11 设A与B为主理想环R上的两个$m\times n$矩阵．则有
A与B相抵$\Longleftrightarrow A$ 与B有相同的秩以及相同的初等因子组．▮

习　　题

1．设 R是有恒等元素的交换环．

1）如果乘积AB可以定义，那么乘积 $B'A'$也可以定义，并且

$$(AB)'=B'A'.$$

2）如果A可逆，那么A'也可逆，并且

$$(A')^{-1}=(A^{-1})'.$$

3）如果 R不是交换环，那么1）与2）可能不成立．

2．设 R 为有恒等元素的环．一个 n 阶方阵 $A=(a_{ij})\in M_n(R)$ 叫做严格上三角形矩阵，是指

$$a_{ij}=0,\ j\leqslant i$$

证明$M_n(R)$ 中一切严格上三角形矩阵组成的子集 N是子环 T 的一个理想，并决定商环 T/N的结构，其中T是 $M_n(R)$ 中一切上三角形矩阵做成的子环．

3．设 R为有恒等元素的环．

1）全阵环$M_n(R)$ 的中心为 $\{rI_n|r$属于R的中心$\}$．

2）$M_n(R)$ 的中心同构于R的中心．

4．矩阵 $A\in M_n(R)$ 叫做是对称的，是指 $A=A'$；叫做是反对称的，是指 $A=-A'$．那么

1）如果A, B都是对称的（或者是反对称的），则$A+B$也

是对称的（或是反对称的）.

2）设 R为交换环．如果A与B是对称的，那么AB 是对称的 $\Longleftrightarrow AB=BA$。

3）对任意的$B\in M_n(R)$，都有BB'与$B+B'$ 均为对称的，而 $B-B'$是反对称的。

5．设 R为有恒等元素的交换环。

1）如果对于 R 中每一个非零元素 r，都有 $r+r\neq 0$．证明：模M上的 n 重线性型：$M^{(n)}\longrightarrow R$ 是交错的$\Longleftrightarrow$它是反对称的。如果环 R的特征数等于 2，结果怎样？

2）如果 $m>n$，那么 $(R^{(n)})^{(m)}$ 上每一个交错的 m 重线性型均为零；如果$m<n$，那么在 $(R^{(n)})^{(m)}$ 上存在有非零的交错的线性型。

3）$A\in M_n(R)$，证明：

$$|A^*|=|A|^{n-1}; \qquad (A^*)^*=|A|^{n-2}A.$$

4）如果R是域，A，$B\in M_n(R)$．证明：除了有限个$r\in R$之外，$A+rB$均为可逆的。

5）设 $(b_1,b_2,\cdots,b_n)$ 是 R上的齐次线性方程组

$$\begin{cases} a_{11}x_1+a_{12}x_2+\cdots+a_{1n}x_n=0, \\ a_{21}x_1+a_{22}x_2+\cdots+a_{2n}x_n=0, \\ \cdot \quad \cdot \quad \cdot \quad \cdots \quad \cdot \quad \cdot \\ a_{n1}x_1+a_{n2}x_2+\cdots+a_{nn}x_n=0, \end{cases}$$

的一组解，$A=(a_{ij})$ 为其系数矩阵．证明：

$$|A|b_i=0, \quad i=1, 2, \cdots, n.$$

6．求整数环 Z上矩阵

$$\begin{pmatrix} 6 & 2 & 3 & 0 \\ 2 & 3 & -4 & 1 \\ -3 & 3 & 1 & 2 \\ -1 & -2 & -3 & 5 \end{pmatrix}$$

的标准形。

7．求$Q[\lambda]$上的矩阵

$$A=\begin{pmatrix}\lambda+1 & 2 & -6\\ 1 & \lambda & -3\\ 1 & 1 & \lambda-4\end{pmatrix}$$

的不变因子，行列式因子。并求 P 与 Q，使得 PAQ 成为标准形阵。

8．设 D为欧氏环。$A\in M_n(D)$，$|A|\neq 0$。证明：存在 D 上可逆矩阵P，使PA成三角形矩阵：

$$PA=\begin{pmatrix}d_1 & b_{12} & b_{13} & \cdots & b_{1n}\\ 0 & d_2 & b_{23} & \cdots & b_{2n}\\ \cdot & \cdot & \cdot & \cdots & \cdot\\ 0 & 0 & 0 & \cdots & d_n\end{pmatrix}$$

9．设M为R—模。对于M中的两组元素：

$$\alpha_1,\alpha_2,\cdots,\alpha_n;\ \beta_1,\beta_2,\cdots,\beta_m,$$

如果有以下的线性关系：

$$\begin{cases}\beta_1=a_{11}\alpha_1+a_{12}\alpha_2+\cdots+a_{1n}\alpha_n,\\ \beta_2=a_{21}\alpha_1+a_{22}\alpha_2+\cdots+a_{2n}\alpha_n,\\ \quad\vdots\\ \beta_m=a_{m1}\alpha_1+a_{m2}\alpha_2+\cdots+a_{mn}\alpha_n,\end{cases}$$

则可简记为矩阵形式：

$$\begin{pmatrix}\beta_1\\ \beta_2\\ \vdots\\ \beta_m\end{pmatrix}=\begin{pmatrix}a_{11} & a_{12} & \cdots & a_{1n}\\ a_{21} & a_{22} & \cdots & a_{2n}\\ \cdot & \cdot & \cdots & \cdot\\ a_{m1} & a_{m2} & \cdots & a_{mn}\end{pmatrix}\begin{pmatrix}\alpha_1\\ \alpha_2\\ \vdots\\ \alpha_n\end{pmatrix}$$

于是有以下的计算规则；

(1)

$$(A+B)\begin{pmatrix}\alpha_1\\ \alpha_2\\ \vdots\\ \alpha_n\end{pmatrix}=A\begin{pmatrix}\alpha_1\\ \alpha_2\\ \vdots\\ \alpha_n\end{pmatrix}+B\begin{pmatrix}\alpha_1\\ \alpha_2\\ \vdots\\ \alpha_n\end{pmatrix},$$

(2)

$$A\left[\begin{pmatrix}\alpha_1\\ \alpha_2\\ \vdots\\ \alpha_n\end{pmatrix}+\begin{pmatrix}\alpha_1'\\ \alpha_2'\\ \vdots\\ \alpha_n'\end{pmatrix}\right]=A\begin{pmatrix}\alpha_1\\ \alpha_2\\ \vdots\\ \alpha_n\end{pmatrix}+A\begin{pmatrix}\alpha_1'\\ \alpha_2'\\ \vdots\\ \alpha_n'\end{pmatrix},$$

(3)

$$(AB)\begin{pmatrix}\alpha_1\\ \alpha_2\\ \vdots\\ \alpha_n\end{pmatrix}=A\left(B\begin{pmatrix}\alpha_1\\ \alpha_2\\ \vdots\\ \alpha_n\end{pmatrix}\right),$$

(4)

$$(kA)\begin{pmatrix}\alpha_1\\ \alpha_2\\ \vdots\\ \alpha_n\end{pmatrix}=k\left(A\begin{pmatrix}\alpha_1\\ \alpha_2\\ \vdots\\ \alpha_n\end{pmatrix}\right).$$

§2 自由模及其秩数

我们已知道有限生成模的概念，环 R 上的模 M 是有限生成的，就是说存在有限个元素α_1，α_2，…，$\alpha_n \in M$，使得

$$M = LC(\alpha_1, \alpha_2, \cdots, \alpha_n) = \{k_1\alpha_1 + k_2\alpha_2 + \cdots + k_n\alpha_n \mid k_i \in R\},$$

此中之 α_1，α_2，…，α_n叫做M的一组生成元素。于是，R—模M是以 α_1，α_2，…，α_n为生成元素的有限生成模$\Longleftrightarrow$$M$ 是循环模的和：

$$M = R\alpha_1 + R\alpha_2 + \cdots + R\alpha_n \qquad (1)$$

我们进一步考察这个和（1）。一般来说它未必是直和，而和（1）是直和$\Longleftrightarrow$模M中之零元素的表示法是唯一的，即

$$k_1\alpha_1 + k_2\alpha_2 + \cdots + k_n\alpha_n = 0 \Longleftrightarrow k_i\alpha_i = 0, \quad i = 1, 2, \cdots, n.$$

当然，$k_i = 0$时，必有 $k_i\alpha_i = 0$。不过反过来则未必。即由$k_i\alpha_i = 0$不能肯定的得出$k_i = 0$。

以上讨论表明：

首先，M是以α_1，α_2，…，α_n为生成元素的有限生成模$\Longleftrightarrow$$M$是循环模$R\alpha_1$，$R\alpha_2$，…，$R\alpha_n$的和，即$M$中每一个元素均可表成$R\alpha_1$，$R\alpha_2$，…，$R\alpha_n$中元素之和的形式：

$\forall \beta \in M$，存在$k_i\alpha_i \in R\alpha_i$，使得

$$\beta = k_1\alpha_1 + k_2\alpha_2 + \cdots + k_n\alpha_n \qquad (2)$$

其次，当和（1）是直和时，β 的表示式（2）是唯一的，即若有

$$\begin{aligned}\beta &= k_1\alpha_1 + k_2\alpha_2 + \cdots + k_n\alpha_n \\ &= k_1'\alpha_1 + k_2'\alpha_2 + \cdots + k_n'\alpha_n\end{aligned}$$

则有

$$k_i\alpha_i = k_i'\alpha_i, \quad i = 1, 2, \cdots, n \qquad (3)$$

最后，如果和（1）是直和，从而表示式（2）是由各加项所唯一决定的，此时，表示式（2）的这种唯一性与其中之各系数k_1，k_2，…，k_n的唯一性还不是一回事情。

诚然，我们容易理解，如果表示式（2）是由它的系数k_1，k_2，…，k_n唯一决定的，那么有限生成模$M = LC(\alpha_1, \alpha_2, \cdots, \alpha_n)$比起一般的直和

$$M = R\alpha_1 \oplus R\alpha_2 \oplus \cdots \oplus R\alpha_n$$

就更加简单，同时也有其突出的重要意义。对此，我们给出如下的基本概念。

定义 1 设M是有限生成的R—模。如果M有一组生成元素α_1，α_2，…，α_n，使得当

$$0 = k_1\alpha_1 + k_2\alpha_2 + \cdots + k_n\alpha_n$$

时，必须每一个系数都是环R中的零元素，即必须

$$k_1 = 0, \ k_2 = 0, \ \cdots, \ k_n = 0,$$

则称M是R上的自由模。生成组α_1，α_2，…，α_n叫做自由模M的一个有序基底，记作$M = [\alpha_1, \alpha_2, \cdots, \alpha_n]$。

例 1 整数加法群$M = \{Z; +\}$做为Z—模是自由模，1是它的一个基底：$M = Z = [1]$。

例 2 剩余类加法群$Z_6 = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}, \overline{5}\}$，做为$Z$—模不是自由模，这是因为$Z_6$中任意非零元素$\overline{i}$都有

$$6 \cdot \overline{i} = \overline{0}$$

由此可知有限生成Z—模Z_6不存在基底，所以它不是整数环Z上的自由模。

但是，Z_6又可以看做剩余类环Z_6上的模。这时生成元素$\overline{1}$是Z_6—模Z_6的一个基底：$Z_6 = [\overline{1}]$，即在环Z_6上看，加法群Z_6是自由模。

例 3 对于任意一个有恒等元素的环R，把加法群$\{R; +\}$看做R—模时，总是自由模，而且$R = [1]$，1是环R的恒等元素。

一般地，直和

$$R^{(n)}=R\oplus R\oplus\cdots\oplus R=\{(x_1,\ x_2,\cdots,x_n)\mid x_i\in R\}$$

也是环 R上的自由模，而且

$$\varepsilon_1=(1,\ 0,\ 0,\ \cdots,\ 1),$$
$$\varepsilon_2=(0,\ 1,\ 0,\ \cdots,\ 0),$$
$$\vdots$$
$$\varepsilon_n=(0,\ 0,\ 0,\ \cdots,\ 1),$$

是$R^{(n)}$的一个有序基：$R^{(n)}=[\varepsilon_1,\ \varepsilon_2,\ \cdots,\ \varepsilon_n]$。

更一般地，$M=\{M_{m\times n}(R);\ +\}$是环$R$上的自由模。"矩阵单位"：

$$E_{ij},\ i=1,\ 2,\ \cdots,\ m;\ j=1,\ 2,\ \cdots,\ n,$$

是自由模$M_{m\times n}(R)$ 的一个基底。其中E_{ij}是这样的$m\times n$矩阵，它的（i, j）位置的元素是环R的恒等元素 1，其余位置的元素均为 0。

例 4 如果M_1，M_2都是 R上的自由模，令

$$\alpha_1,\ \alpha_2,\ \cdots,\ \alpha_r\text{与 }\beta_1,\ \beta_2,\ \cdots,\ \beta_S$$

分别是M_1与M_2的一个有序基，那么直和

$$M=M_1\oplus M_2$$

也是 R上的自由模，并且

$$\alpha_1,\ \alpha_2,\ \cdots,\ \alpha_r,\ \beta_1,\ \beta_2,\ \cdots,\ \beta_S$$

就是直和M的一个有序基，即

$$M=[\alpha_1,\ \alpha_2,\ \cdots,\ \alpha_r,\ \beta_1,\ \beta_2,\ \cdots,\ \beta_S]$$

亦即

$$[\alpha_1,\alpha_2,\cdots,\alpha_r]\oplus[\beta_1,\beta_2,\cdots,\beta_S]$$
$$=[\alpha_1,\alpha_2,\cdots,\alpha_r,\beta_1,\beta_2,\cdots,\ \beta_S]$$

事实上不难看出 α_1，α_2，$\cdots$，α_r,β_1,β_2,$\cdots$，β_S是直和$M=M_1\oplus M_2$的一组生成元素。于是，如果

$$0=k_1\alpha_1+k_2\alpha_2+\cdots+k_r\alpha_r+l_1\beta_1+l_2\beta_2+\cdots+l_S\beta_S$$

根据直和的性质，可得

$$k_1\alpha_1+k_2\alpha_2+\cdots+k_r\alpha_r=0,$$

$$l_1\beta_1 + l_2\beta_2 + \cdots + l_S\beta_S = 0$$

又因为 $\alpha_1, \alpha_2, \cdots, \alpha_r$; $\beta_1, \beta_2, \cdots, \beta_S$均为自由模的基底，所以即有

$$k_1 = 0, k_2 = 0, \cdots, k_r = 0, l_1 = 0, l_2 = 0, \cdots, l_S = 0.$$

这就说明 $\alpha_1, \alpha_2, \cdots, \alpha_r, \beta_1, \beta_2, \cdots, \beta_S$是模$M$的一个基底，$M = M_1 \oplus M_2$是自由模。

例 5 设$M = Z \oplus Z_6$。那么M不是整数环Z上的自由模。

事实上，直和$M = Z \oplus Z_6$中任何一个元素 $\alpha = (a, b)$ 显然不能做成基底。进而，令

$$\alpha_1 = (a_1, b_1), \quad \alpha_2 = (a_2, b_2)$$

为M中的任意两个元素，而且不妨认为 $a_1 \neq 0$。于是，取

$$k_1 = -6a_2, \quad k_2 = 6a_1 \neq 0,$$

则有

$$\begin{aligned} k_1\alpha_1 + k_2\alpha_2 &= k_1(a_1, b_1) + k_2(a_2, b_2) \\ &= (k_1a_1 + k_2a_2,\ k_1b_1 + k_2b_2) \\ &= (-6a_2a_1 + 6a_1a_2,\ -6a_2b_1 + 6a_1b_2) \\ &= (0, \overline{0}). \end{aligned}$$

这说明α_1, α_2表出 $(0, \overline{0})$ 的方法不是唯一的，故而α_1，α_2不可能成为模M的基底。由此便可肯定直和 $M = Z \oplus Z_6$的任意一组元素

$$\alpha_1, \alpha_2, \cdots, \alpha_r$$

均不可能做成M的基底，即知 $M = Z \oplus Z_6$不是Z上的自由模。

例 6 域 F上的有限维线性空间 V，做为F—模是自由模，而且V中一组向量

$$\alpha_1, \alpha_2, \cdots, \alpha_n$$

是 F 上自由模 V的基底$\Longleftrightarrow \alpha_1, \alpha_2, \cdots, \alpha_n$ 是线性空间V的基底。

此外，我们知道，任意取定n维线性空间V的一个线性变换σ之后，便可由 σ 诱导出多项式环$F[\lambda]$ 上的模 V，换句话说就是在

原来域F上的线性空间V的加法群的基础上，通过线性变换σ的作用使加法群V成为多项式环$F[\lambda]$上的模。这时的倍数乘法规定为

$$f(\lambda)\alpha = f(\sigma)(\alpha), \quad \forall f(\lambda)\in F[\lambda], \alpha\in V.$$

于是，对$F[\lambda]$—模V中的任意一个元素α，则有

$$\sigma^0(\alpha)=\alpha,\ \sigma(\alpha),\ \sigma^2(\alpha),\cdots,\sigma^m(\alpha),$$

是线性空间V中的一组元素，共有$m+1$个元素。因为V关于域F的维数等于n，所以V中凡是多于n个元素的一组元素必是线性相关的，从而，当$m\geqslant n$时，上述的那组$m+1$个元素就是线性相关的。即存在域F中的$m+1$个元素

$$a_0,\ a_1,\ a_2,\cdots,a_m$$

不全是零元素，使得

$$a_0\alpha + a_1(\sigma(\alpha)) + a_2(\sigma^2(\alpha)) + \cdots + a_m(\sigma^m(\alpha)) = 0$$

亦即

$$(a_0 + a_1\sigma + a_2\sigma^2 + \cdots + a_m\sigma^m)\ (\alpha) = 0$$

若令

$$f(\lambda) = a_0 + a_1\lambda + a_2\lambda^2 + \cdots + a_m\lambda^m$$

便有

$$f(\lambda)\alpha = 0,$$

而且$f(\lambda)\neq 0$，这就说明，由线性变换σ所导出的$F[\lambda]$—模V不可能是自由模。

明显可见，环R上的自由模是域F上有限维线性空间概念的直接推广。只是这里没使用线性无关与线性相关这样的术语。当然，对于一般的R—模M可以完全类似的规定一组元素的线性相关性的概念，即R—模M中的一组元素

$$\alpha_1,\ \alpha_2,\ \cdots,\ \alpha_s$$

如果存在环R中的s个不全为零的元素k_1，k_2，$\cdots$，k_S，使得

$$k_1\alpha_1 + k_2\alpha_2 + \cdots + k_S\alpha_S = 0,$$

则称$\alpha_1,\alpha_2,\cdots,\alpha_S$关于$R$是线性相关的，否则，就说$\alpha_1,\alpha_2,\cdots,\alpha_S$关于$R$是线性无关的。这样，$R$—模$M$的一组元素$\alpha_1,\alpha_2,\cdots,$

α_S 关于 R是线性无关的充分必要条件是

$$k_1\alpha_1+k_2\alpha_2+\cdots+k_S\alpha_S=0\Longrightarrow k_1=k_2=\cdots=k_S=0.$$

由此可见，R—模M是自由模$\Longleftrightarrow M$有一组线性无关的生成元素。换个说法，α_1，α_2，$\cdots$，α_S是模M的一个基底$\Longleftrightarrow\alpha_1$，$\alpha_2$，$\cdots$，$\alpha_S$是$M$的一组线性无关的生成元素。

值得注意的是一般 R—模M中元素之间的线性关系与特殊的模，域F上线性空间V的向量之间的线性关系是有很大差异的。例如，在域F上的n维线性空间V中，总有

1）$k\alpha=0\Longleftrightarrow k=0$ 或是$\alpha=0$；任一非零元素α必是线性无关的。

2）若α_1，α_2，$\cdots$，α_S（$s\geqslant 2$）是线性相关的$\Longrightarrow$至少有一个α_i能用其余的α_1，$\cdots$，α_{i-1}，α_{i+1}，$\cdots$，α_S线性表出。

3）若α_1，α_2，$\cdots$，α_S线性无关，而α_1，α_2，$\cdots$，α_S，β线性相关$\Longrightarrow\beta$一定能用α_1，α_2，$\cdots$，α_S线性表出。

4）V的子空间也是有限维的，并且真子空间的维数必小于n。

5）V中任意一组线性无关元素必能扩充成为V的一个基底。

诚然，以上这些熟知的基本事实对于线性空间理论来说是非常重要的。但是，但于一般的自由R—模来说都已不是普遍的规律了。

下面指出自由模的一些简单的基本的性质。

命题 1 R—模M是有限生成的$\Longleftrightarrow M$是自由R—模的同态象。从而与自由模的商模是同构的。

证 设R—模M是有限生成的。令

$$\alpha_1,\ \alpha_2,\ \cdots,\ \alpha_n$$

是M的任意一组生成元素。即有

$$\begin{aligned}M&=LC(\alpha_1,\ \alpha_2,\ \cdots,\ \alpha_n)\\&=\{k_1\alpha_1+k_2\alpha_2+\cdots+k_n\alpha_n\,|\,k_i\in R\}\end{aligned}$$

于是，我们用 R—模$R^{(n)}=\{(x_1, x_2, \cdots, x_n)|x_i\in R\}$与有限生成模$M$做比较．这里模$R^{(n)}$是$R$上的自由模．规定映射：

$$\varphi:(x_1, x_2, \cdots, x_n)\longmapsto x_1\alpha_1+x_2\alpha_2+\cdots+x_n\alpha_n,$$

显然，做为映射规则φ是合理的，并且是到M上的满射．进而容易验算，当又有

$$\varphi:(y_1, y_2,\cdots,y_n)\longmapsto y_1\alpha_1+y_2\alpha_2+\cdots+y_n\alpha_n$$

时，则有

$$\varphi((x_1,\cdots,x_n)+(y_1,\cdots,y_n))=\varphi((x_1,\cdots,x_n))+\varphi((y_1,\cdots,y_n)),$$

$$\varphi\ (k(x_1,x_2,\cdots,x_n))\ =k\varphi\ ((x_1,x_2,\cdots,x_n))$$

即φ是一个模同态．从而

$$R^{(n)}\overset{\varphi}{\sim}M,$$

由模同态基本定理，又有

$$R^{(n)}\Big/ker\varphi\overset{\bar{\varphi}}{\simeq}M,$$

其中$\bar{\varphi}(\overline{(x_1,\cdots,x_n)})=\varphi((x_1,\cdots,x_n)),\forall\overline{(x_1\cdots x_n)}\in R^{(n)}\Big/ker\varphi$

这就证明了命题1的必要性．

反之，如果有自由模N，使得模M是N的同态象，可令

$$N\overset{\psi}{\sim}M$$

于是，任取自由模N的一个基底：$\varepsilon_1, \varepsilon_2, \cdots, \varepsilon_n$考虑基底元素$\varepsilon_i$（$i=1, 2, \cdots, n$）在同态映射$\psi$之下的象，则有

$$\psi(\varepsilon_1)=\alpha_1,\ \psi(\varepsilon_2)=\alpha_2,\ \cdots,\ \psi(\varepsilon_n)=\alpha_n,$$

这样不难验证：$M=LC(\alpha_1, \alpha_2, \cdots, \alpha_n)$，即$M$是以$\alpha_1, \alpha_2, \cdots, \alpha_n$为一组生成元素的有限生成模．

这又证明了命题1的充分性．▮

为了从不同的角度认识自由模的特性，我们指出如下的

命题 2 设M是环R上的模，$M\neq\{0\}$,那么以下各条是等价的：

（1）M是自由R—模；

（2）M有一个在 R上线性无关的生成组；

（3）M中存在一组元素 $\alpha_1,\alpha_2,\cdots,\alpha_n$，使得$M$中的每一个元素$\beta$都能唯一地表成$\alpha_1,\alpha_2,\cdots,\alpha_n$的线性组合：

$$\beta=k_1\alpha_1+k_2\alpha_2+\cdots+k_n\alpha_n,$$

其中 k_1，k_2，…，$k_n\in R$，是由β唯一决定的；

（4）M是一些循环模的直和：

$$M=R\alpha_1\oplus R\alpha_2\oplus\cdots\oplus R\alpha_n,$$

其中 $ann\alpha_i=0$，且只少有一个$\alpha_i\neq 0$，$i=1,2,\cdots,n$；

（5）对于某一个 n，使得

$$M\simeq R^{(n)}=R\oplus R\oplus\cdots\oplus R.$$

命题 2 的证明，做为习题留给读者去做．▌

我们知道，自由模按定义自然都是有限生成的．但是反过来，有限生成模未必准是自由模．既使对于相当特殊的环 R来说也是如此，比如主理想环 R上的有限生成模可以不是自由模．不过，如所周知，当 R是域时，域 R 上的自由模M（即M是有限维线性空间）与M是有限生成的就是一回事情了．进而，我们还可以指出较为一般的结果，即有

定理 1 设 R为除环（也叫体）．则有，R—模 M是自由的$\Longleftrightarrow M$是有限生成的．

证 必要性是自明的．现在证明充分性．即已知M是有限生成模，往证M是自由 R—模．

任取M的一个生成组：$\alpha_1,\alpha_2,\cdots,\alpha_n$，令

$$S=\{\alpha_1,\ \alpha_2,\ \cdots,\ \alpha_n\},$$

做为M的一个子集来考虑，看由 S 中的元素所组成的线性无关的子集．显然，所有这些成线性无关的子集的每一个，所含元素个数都 $\leqslant n$．从而其中必有包含元素的个数较多的．任取其一，设为

$$S'=\{\alpha_{i_1},\alpha_{i_2},\cdots,\alpha_{i_r}\},$$

其中 $1\leqslant i_1<i_2<\cdots<i_r\leqslant n$．

于是，不难指出 $\alpha_{i_1},\alpha_{i_2},\cdots,\alpha_{i_r}$ 就是模M的一个基底。

首先，$\alpha_{i_1},\alpha_{i_2},\cdots,\alpha_{i_r}$ 也是M的一个生成组，为此，关键在于说明S中的每一个元素都能用 $\alpha_{i_1},\alpha_{i_2},\cdots,\alpha_{i_r}$ 线性表出就足够了。令$\alpha_j\in S-S'$。于是，由S'的取法，即S'是S的含有线性无关元素最多的一个子集。从而

$$S'\cup\{\alpha_j\}$$

必是线性相关的。故有

$$k_1\alpha_{i_1}+k_2\alpha_{i_2}+\cdots+k_r\alpha_{i_r}+k\alpha_j=0,$$

而且 $k_1,k_2,\cdots,k_r,k$ 不全为零。特别地，$k\neq 0$ 否则将与 α_{i_1}，$\alpha_{i_2},\cdots,\alpha_{i_r}$ 是线性无关的相矛盾。这样，k就是除环 R中的一个非零元素，因而存在逆元 $k^{-1}\in R$。由此便得

$$\alpha_j=k^{-1}(-k_1)\alpha_{i_1}+k^{-1}(-k_2)\alpha_{i_2}+\cdots+k^{-1}(-k_r)\alpha_{i_r}$$

由线性表出的传递性，α_{i_1}，α_{i_2}，$\cdots$，α_{i_r}也是M的一组生成元素，即$M=LC(\alpha_{i_1},\ \alpha_{i_2},\ \cdots,\ \alpha_{i_r})$。再由命题2，可知$\alpha_{i_1},\alpha_{i_2}$，$\cdots$，$\alpha_{i_r}$是$M$的一个基底，即得

$$M=[\alpha_{i_1},\ \alpha_{i_2},\ \cdots,\ \alpha_{i_r}].\ \blacksquare$$

推论 1 设M是除环R上的自由模，那么M的任意一个生成组$S=\{\alpha_1,\alpha_2,\cdots,\alpha_n\}$中都包含有$M$的一组基底。█

推论 2 设M是除环R上的自由模，那么M的任意一组线性无关元素α_1，α_2，$\cdots$，α_r都含在M的一个基底之中。换句话说，M的任意一组线性无关元素α_1，α_2，$\cdots$，α_r都可以扩充成M的一个基底。特别地，M的任意一个极大线性无关组（定义同高等代数）必为M的一个基底，反之亦然。█

容易理解，自由模M的重要意义在于它有有限个元素组成的基底。明显的是一个自由R—模M会有许多不同的基底。这样就出现一个问题，一个自由R—模M的各个基底中所含元素的个数

是否都一样多？当然，如所周知，对于非常特殊的自由模来说——域F上的自由模V是这样的，通常把这样的重要事实叫做"维数不变性"，即域具有"维数不变性"．遗憾的是，对于一般的环来说不再具有这种"维数不变性"．不过好在对于许多常见的环R来说都具有这种非常重要的特性：环R上每一个自由模M的一切基底中所含元素的个数都一样．这就是我们将要证明的

定理 2 设R为有恒等元素的交换环，M是R上的自由模．如果$\alpha_1,\alpha_2,\cdots,\alpha_n$与$\beta_1,\beta_2,\cdots,\beta_m$都是$M$的基底，那么$m=n$。

证 因为$\alpha_1,\alpha_2,\cdots,\alpha_n$与$\beta_1,\beta_2,\cdots,\beta_m$都是$M$的基底，则有

$$\begin{cases}\alpha_1=a_{11}\beta_1+a_{12}\beta_2+\cdots+a_{1m}\beta_m,\\ \alpha_2=a_{21}\beta_1+a_{22}\beta_2+\cdots+a_{2m}\beta_m,\\ \cdot\quad\cdot\quad\cdot\quad\cdot\quad\cdots\quad\cdot\\ \alpha_n=a_{n1}\beta_1+a_{n2}\beta_2+\cdots+a_{nm}\beta_m.\end{cases}$$

$$\begin{cases}\beta_1=b_{11}\alpha_1+b_{12}\alpha_2+\cdots+b_{1n}\alpha_n,\\ \beta_2=b_{21}\alpha_1+b_{22}\alpha_2+\cdots+b_{2n}\alpha_n,\\ \cdot\quad\cdot\quad\cdot\quad\cdot\quad\cdots\quad\cdot\\ \beta_m=b_{m1}\alpha_1+b_{m2}\alpha_2+\cdots+b_{mn}\alpha_n.\end{cases}$$

其中 $a_{ij}\in R,b_{ji}\in R$。

令$A=(a_{ij}),B=(b_{ji})$，即$A\in M_{n\times m}(R)$，$B\in M_{m\times n}(R)$。于是，根据$\alpha_1,\alpha_2,\cdots,\alpha_n$与$\beta_1,\beta_2,\cdots,\beta_m$都是模$M$的基底的性质，可得

$$AB=I_n,\qquad BA=I_m.$$

假设 $m<n$，令

$$A_1=\begin{pmatrix}A & 0_{n\times(n-m)}\end{pmatrix},\quad B_1=\begin{pmatrix}B\\ 0_{(n-m)\times n}\end{pmatrix}$$

这样，A_1与B_1都成了n阶方阵，且有

$$A_1B_1=I_n.$$

因为R是有恒等元素的交换环，由上一节的定理6之推论3，可

知A_1是可逆的，并且B_1就是A_1的逆阵。从而也有

$$B_1A_1=I_n$$

但是，容易计算

$$B_1A_1=\begin{pmatrix} B \\ 0_{(n-m)\times n}\end{pmatrix}\begin{pmatrix} A & 0_{n\times(n-m)}\end{pmatrix}$$

$$=\begin{pmatrix} BA & 0_{m\times(n-m)} \\ 0_{(n-m)\times m} & 0_{(n-m)\times(n-m)}\end{pmatrix}.$$

由于假设 $m<n$，使得 B_1A_1 不可能等于 n 阶单位阵 I_n。从而说明，必有 $m\geqslant n$。同理可得 $n\geqslant m$。所以$m=n$。█

这个定理断定，对于有恒等元素的交换环 R来说，R 上任意的自由模M的基底中所含元素的个数是一个唯一确定的数。于是我们可以给出相当于线性空间的维数的概念。

定义 2 设R为有恒等元素的交换环，M为R上的自由模。称自由模M的基底中所含元素的个数n为M的秩数，记作$rankM=n$。同时也称M是 n 秩自由模。特别地，把零模也叫做自由模，并约定零模的秩数为 0 .

例如，令R为以 6 为模的剩余类环Z_6，取 $M=\{Z_6;\ +\}$. 于是，$M=[\bar{1}]$，因而M是Z_6上秩数等于 1 的自由模。

再如，对任意的有恒等元素的交换环R来说，$R^{(n)}$ 恰是 R上的 n 秩自由模。如所周知，如下的 n 个元素：

$$\varepsilon_1=(1,0,0,\cdots,0),$$
$$\varepsilon_2=(0,1,0,\cdots,0),$$
$$\cdots\quad\cdots\quad\cdots\quad\cdots\quad\cdots$$
$$\varepsilon_n=(0,0,0,\cdots,1)$$

是 $R^{(n)}$ 的一个有序基底，通常称其为 $R^{(n)}$ 的自然基底或标准基底。

显然，对于域 F上的有限维线性空间来说，秩数就是维数。

与线性空间一样，若M是R上的n秩自由模，那么M中的一组

元素能成为M的一个基底必须是恰好含有 n 个元素。当然，并不是凡 n 个元素就一定成为M的一个基底。

定理 3 设M是交换环R上的n秩自由模。$\alpha_1,\alpha_2,\cdots,\alpha_n$是$M$的一个基底，$\beta_1,\beta_2,\cdots,\beta_n$是$M$的任意 n 个元素，令

$$\begin{cases}\beta_1=t_{11}\alpha_1+t_{12}\alpha_2+\cdots+t_{1n}\alpha_n,\\ \beta_2=t_{21}\alpha_1+t_{22}\alpha_2+\cdots+t_{2n}\alpha_n,\\ \qquad\vdots\\ \beta_n=t_{n1}\alpha_1+t_{n2}\alpha_2+\cdots+t_{nn}\alpha_n.\end{cases}$$

则有，$\beta_1,\beta_2,\cdots,\beta_n$也是$M$的一个基底$\Longleftrightarrow n$ 阶方阵 $T(t_{ij})$ 是可逆的。

证 先证明充分性成立，为了简便，我们也采取高等代数中使用过的记法，即把每一个β_i用$\alpha_1,\alpha_2,\cdots,\alpha_n$线性表出的式子集中的写成矩阵形式：

$$\begin{pmatrix}\beta_1\\ \beta_2\\ \vdots\\ \beta_n\end{pmatrix}=T\begin{pmatrix}\alpha_1\\ \alpha_2\\ \vdots\\ \alpha_n\end{pmatrix}$$

这样，因为T是可逆的，存在逆阵 T^{-1}。用 T^{-1}从左边去乘上式的两端，则得

$$T^{-1}\begin{pmatrix}\beta_1\\ \beta_2\\ \vdots\\ \beta_n\end{pmatrix}=T^{-1}\left[T\begin{pmatrix}\alpha_1\\ \alpha_2\\ \vdots\\ \alpha_n\end{pmatrix}\right]$$

$$=(T^{-1}T)\begin{pmatrix}\alpha_1\\ \alpha_2\\ \vdots\\ \alpha_n\end{pmatrix}$$

$$=\begin{pmatrix}\alpha_1\\ \alpha_2\\ \vdots\\ \alpha_n\end{pmatrix}$$

这说明每一个α_i（$i=1,2,\cdots,n$）均可由$\beta_1,\beta_2,\cdots,\beta_n$线性表出。因为$\alpha_1,\alpha_2,\cdots,\alpha_n$是$M$的基底，所以$\beta_1,\beta_2,\cdots,\beta_n$是$M$的一组生成元素。

进而，为了证明$\beta_1,\beta_2,\cdots,\beta_n$也是$M$的一个基底。只要指出$\beta_1,\beta_2,\cdots,\beta_n$关于$R$是线性无关的就行了。令

$$d_1\beta_1+d_2\beta_2+\cdots+d_n\beta_n=\sum_{i=1}^{n}d_i\beta_i=0.$$

将每一个β_i用其由$\alpha_1,\alpha_2,\cdots,\alpha_n$的表示式代换进去，则有

$$\begin{aligned}0&=d_1\beta_1+d_2\beta_2+\cdots+d_n\beta_n\\&=d_1(t_{11}\alpha_1+t_{12}\alpha_2+\cdots+t_{1n}\alpha_n)+\\&\quad+d_2(t_{21}\alpha_1+t_{22}\alpha_2+\cdots+t_{2n}\alpha_n)+\\&\quad+\cdots+\\&\quad+d_n(t_{n1}\alpha_1+t_{n2}\alpha_2+\cdots+t_{nn}\alpha_n)\\&=(d_1t_{11}+d_2t_{21}+\cdots+d_nt_{n1})\alpha_1+\\&\quad+(d_1t_{12}+d_2t_{22}+\cdots+d_nt_{n2})\alpha_2+\\&\quad+\cdots+\\&\quad+(d_1t_{1n}+d_2t_{2n}+\cdots+d_nt_{nn})\alpha_n,\end{aligned}$$

因为$\alpha_1,\alpha_2,\cdots,\alpha_n$是基底，所以

$$\begin{cases}d_1t_{11}+d_2t_{21}+\cdots+d_nt_{n1}=0,\\ d_1t_{12}+d_2t_{22}+\cdots+d_nt_{n2}=0,\\ \cdot\quad\cdot\quad\cdot\quad\cdots\quad\cdots\\ d_1t_{1n}+d_2t_{2n}+\cdots+d_nt_{nn}=0.\end{cases}$$

把上述这n个等式改写成矩阵的形式，即为

$$(d_1 d_2 \cdots d_n)\begin{pmatrix} t_{11} & t_{12} & \cdots & t_{1n} \\ t_{21} & t_{22} & \cdots & t_{2n} \\ \cdot & \cdot & \cdots & \cdot \\ t_{n1} & t_{n2} & \cdots & t_{nn} \end{pmatrix} = (0\ 0 \cdots 0)$$

用 $T=(t_{ij})$的逆阵T^{-1}从右端去乘上式两边，则得

$$(d_1 d_2 \cdots d_n) = (0\ 0 \cdots 0),$$

亦即$d_1=0, d_2=0, \cdots, d_n=0$。这就肯定了$\beta_1, \beta_2, \cdots, \beta_n$是线性无关的。总之，$\beta_1, \beta_2, \cdots, \beta_n$是$M$的一个基底。

其次证明必要性成立。已知$\beta_1, \beta_2, \cdots, \beta_n$也是$M$的一个基底，去证$\beta_1, \beta_2, \cdots, \beta_n$用原基底$\alpha_1, \alpha_2, \cdots, \alpha_n$线性表出的系数组成的$n$阶矩阵$T=(t_{ij})$是可逆的。因为$\beta_1, \beta_2, \cdots, \beta_n$也是$M$的基底，所以$\alpha_1, \alpha_2, \cdots, \alpha_n$都能用$\beta_1, \beta_2, \cdots, \beta_n$线性表出，即有

$$\begin{cases} \alpha_1 = t'_{11}\beta_1 + t'_{12}\beta_2 + \cdots + t'_{1n}\beta_n, \\ \alpha_2 = t'_{21}\beta_1 + t'_{22}\beta_2 + \cdots + t'_{2n}\beta_n, \\ \quad \vdots \\ \alpha_n = t'_{n1}\beta_1 + t'_{n2}\beta_2 + \cdots + t'_{nn}\beta_n, \end{cases}$$

亦即

$$\begin{pmatrix} \alpha_1 \\ \alpha_2 \\ \vdots \\ \alpha_n \end{pmatrix} = S\begin{pmatrix} \beta_1 \\ \beta_2 \\ \vdots \\ \beta_n \end{pmatrix},$$

其中$S=(t'_{ij})$于是则有

$$\begin{pmatrix} \alpha_1 \\ \alpha_2 \\ \vdots \\ \alpha_n \end{pmatrix} = ST\begin{pmatrix} \alpha_1 \\ \alpha_2 \\ \vdots \\ \alpha_n \end{pmatrix}$$

由于$\alpha_1, \alpha_2, \cdots, \alpha_n$是$M$的基底，故有

$$ST = I_n.$$

这样，T必为可逆的。▌

定理 3 的意义在于说明，交换环R上的 n 秩自由模 M的基底与R上的可逆 n 阶矩阵是一一相当的．通常把联系着两个基底$\alpha_1,\alpha_2,\cdots,\alpha_n$与$\beta_1,\beta_2,\cdots,\beta_n$的系数矩阵 T：

$$\begin{pmatrix}\beta_1\\ \beta_2\\ \vdots\\ \beta_n\end{pmatrix}=T\begin{pmatrix}\alpha_1\\ \alpha_2\\ \vdots\\ \alpha_n\end{pmatrix}$$

叫做从基底$\alpha_1,\alpha_2,\cdots,\alpha_n$到基底$\beta_1,\beta_2,\cdots,\beta_n$的过渡矩阵。

如果给定了自由模M的两个基底：

$$\alpha_1,\alpha_2,\cdots,\alpha_n;\ \beta_1,\beta_2,\cdots,\beta_n.$$

对于M中的任意一个元素 ν，已知 ν关于基底$\alpha_1,\alpha_2,\cdots,\alpha_n$的表出系数$a_1,a_2,\cdots,a_n$：

$$\nu=a_1\alpha_1+a_2\alpha_2+\cdots+a_n\alpha_n,$$

那么，通过基底的过渡矩阵 T，便可得出元素 ν 关于基底 β_1，，$\cdots,\beta_n$ 的表出系数$b_1,b_2,\cdots,b_n$.

β 事实上，若令

$$\nu=b_1\beta_1+b_2\beta_2+\cdots+b_n\beta_n.$$

写成矩阵形式就是

$$\nu=(b_1b_2\cdots b_n)\begin{pmatrix}\beta_1\\ \beta_2\\ \vdots\\ \beta_n\end{pmatrix}.$$

于是，把各个β_i都用$\alpha_1,\alpha_2,\cdots,\alpha_n$的表示式代换进去，则有

$$\nu=(b_1b_2\cdots b_n)\ T\begin{pmatrix}\alpha_1\\ \alpha_2\\ \vdots\\ \alpha_n\end{pmatrix}.$$

因为元素ν关于基底α_1，α_2，$\cdots$，α_n的表示系数是唯一的，故有

$$(b_1b_2\cdots b_n)T=(a_1a_2\cdots a_n).$$

从而可得

$$(b_1 b_2 \cdots b_n) = (a_1 a_2 \cdots a_n) T^{-1}.$$

这就是同一个元素 v 关于两个基底：

$$\alpha_1, \alpha_2, \cdots, \alpha_n;\ \beta_1,\ \beta_2,\ \cdots,\ \beta_n$$

的表示系数 a_1, a_2, …, a_n与b_1, b_2, …, b_n 之间的关系式. 其中 T是从基底α_1, α_2, …, α_n到基底β_1, β_2, …, β_n的过渡矩阵.

定理 4 设 R为有恒等元素的交换环. 则有，R 上的两个自由模M与M'是同构的充分必要条件是

$$rankM = rankM'.$$

证 先证明充分性成立. 假设 $rankM = rankM'$, 去证 M 与 M'是同构的.

当 $rankM = 0$ 时，则有 $M = \{0\}$, $M' = \{0\}$. 因而自然有 $M \simeq M'$. 一般地，令 $rankM = rankM' = n$, 在 M与M'中分别任意取定一个基底：

$$\alpha_1,\ \alpha_2,\ \cdots,\ \alpha_n \in M;$$
$$\alpha_1',\ \alpha_2',\ \cdots,\ \alpha_n' \in M'.$$

于是，可以规定一个映射

$$\varphi: x_1\alpha_1 + x_2\alpha_2 + \cdots + x_n\alpha_n \longmapsto x_1\alpha_1' + x_2\alpha_2' + \cdots + x_n\alpha_n'.$$

显然，规则φ做为是从M到M'的一个映射是合理的. 并且不难看出，映射φ是到M'上的满射，同时又是单射. 进而，若再有

$$\varphi: y_1\alpha_1 + y_2\alpha_2 + \cdots + y_n\alpha_n \longmapsto y_1\alpha_1' + y_2\alpha_2' + \cdots + y_n\alpha_n',$$

那么，就有

$$\varphi((x_1\alpha_1 + x_2\alpha_2 + \cdots + x_n\alpha_n) + (y_1\alpha_1 + y_2\alpha_2 \cdots + y_n\alpha_n)) =$$
$$= \varphi(x_1\alpha_1 + x_2\alpha_2 + \cdots + x_n\alpha_n) + \varphi(y_1\alpha_1 + y_2\alpha_2 \cdots + y_n\alpha_n);$$
$$\varphi(k(x_1\alpha_1 + x_2\alpha_2 + \cdots + x_n\alpha_n)) = k\varphi(x_1\alpha_1 + x_2\alpha_2 + \cdots + x_n\alpha_n)$$

这就是说，映射 φ是一个模同构映射，即

$$M \overset{\varphi}{\simeq} M'.$$

其次证明必要性成立。假设$M\simeq M'$，去证$rankM=rankM'$。

当$M=\{0\}$时，必有$M'=\{0\}$，从而$rankM=rankM'$。一般地，设$rankM=n>0$，在M中任意取定一个基底：

$$\alpha_1,\ \alpha_2,\ \cdots,\ \alpha_n.$$

由$M\simeq M'$，可令φ是M到M'的一个模同构映射。令

$$\varphi(\alpha_1)=\alpha_1',\ \varphi(\alpha_2)=\alpha_2',\ \cdots,\ \varphi(\alpha_n)=\alpha_n'.$$

于是，对于模M'的任意一个元素β'，必有

$$\beta\in M,\ 使得\beta'=\varphi(\beta).$$

这样，把β用模M的基底α_1，α_2，…，α_n表示出来：

$$\beta=b_1\alpha_1+b_2\alpha_2+\cdots+b_n\alpha_n,$$

则有

$$\begin{aligned}\beta'=\varphi(\beta)&=\varphi(b_1\alpha_1+b_2\alpha_2+\cdots+b_n\alpha_n)\\&=b_1\varphi(\alpha_1)+b_2\varphi(\alpha_2)+\cdots+b_n\varphi(\alpha_n)\\&=b_1\alpha_1'+b_2\alpha_2'+\cdots+b_n\alpha_n'.\end{aligned}$$

由此可知，$\alpha_1',\alpha_2',\cdots,\alpha_n'$是模$M'$的一组生成元素。进而，若有

$$0=b_1\alpha_1'+b_2\alpha_2'+\cdots+b_n\alpha_n',$$

则有

$$\begin{aligned}0&=b_1\alpha_1'+b_2\alpha_2'+\cdots+b_n\alpha_n'\\&=b_1\varphi(\alpha_1)+b_2\varphi(\alpha_2)+\cdots+b_n\varphi(\alpha_n)\\&=\varphi(b_1\alpha_1+b_2\alpha_2+\cdots+b_n\alpha_n),\end{aligned}$$

由于φ是同构映射，则得

$$b_1\alpha_1+b_2\alpha_2+\cdots+b_n\alpha_n=0.$$

又因α_1，α_2，…，α_n是模M的基底，故有

$$b_1=0,\ b_2=0,\ \cdots,\ b_n=0.$$

这就说明，α_1'，α_2'，…，α_n'是线性无关的。总之，α_1'，α_2'，…，α_n'是模M'的一个基底，亦即

$$rankM'=n. \ \blacksquare$$

推论 设R是有恒等元素的交换环。那么，M是R上的$n(>0)$秩自由模$\Longleftrightarrow M\simeq R^{(n)}$。

事实上，这个推论就是定理5的另外一种说法。因此，没有更多要说的话。▌

定理4（或推论）的意义在于，它表明交换环R上的自由模M之代数结构仅仅决定于它的秩数$rankM$。以抽象代数的观点来说，$R^{(n)}$穷尽了交换环R上的自由模（充其量再补充一个零模$M=\{0\}$）。从而可以说，交换环R上的$n(>0)$秩自由模就是R上所有的$1\times n$矩阵，即"n数组"做成的模。

以上介绍了自由模的概念和基本性质。特别是对于交换环R来说，我们证明了所谓的"维数不变性"，从而揭示出交换环R上自由模的数量特征——秩数。

最后，再举一个例子来结束本节的讨论。

例 7 设R为除环，M是R上的自由模。那么，M的任意两个基底中所含元素的个数相等。

证 令

$$\alpha_1, \alpha_2, \cdots, \alpha_n 与 \beta_1, \beta_2, \cdots, \beta_m$$

是M的两个基底。去证$m=n$。

因为$\alpha_1, \alpha_2, \cdots, \alpha_n$与$\beta_1, \beta_2, \cdots, \beta_m$都是$M$的基底，所以$\beta_m\neq 0$，并且

$$\beta_m=r_1\alpha_1+r_2\alpha_2+\cdots+r_n\alpha_n,$$

其中$r_1, r_2, \cdots, r_n\in R$，而且不全等于零。

如果令r_k是第一个不等于零的系数，则有

$$\alpha_k=r_k^{-1}\beta_m-r_k^{-1}r_{k+1}\alpha_{k+1}-\cdots-r_k^{-1}r_n\alpha_n.$$

这表明$\beta_m, \alpha_1, \cdots, \alpha_{k-1}, \alpha_{k+1}, \cdots, \alpha_n$是模$M$的一组生成元素。特别地，

$$\beta_{m-1}=s_m\beta_m+t_1\alpha_1+\cdots+t_{k-1}\alpha_{k-1}+t_{k+1}\alpha_{k+1}+\cdots+t_n\alpha_n$$

其中$s_m\in R$，而且$t_1, \cdots, t_{k-1}, t_{k+1}, \cdots, t_n$不全为零。因为不然的话便有

$$\beta_{m-1}-s_m\beta_m=0,$$

这与$\beta_1, \cdots, \beta_{m-1}, \beta_m$是基底相矛盾。

如果令 t_j 是其中第一个不为零的，则有α_j就可以用β_{m-1}，β_m和 $\{\alpha_i|i\neq j,\ k\}$ 线性表出。这就说明

$$\{\beta_{m-1},\ \beta_m\}\cup\{\alpha_i|i\neq j,\ k\}$$

是模M的一个生成元素集.从而又有，β_{m-2}能用子集 $\{\beta_{m-1},\beta_m\}\cup\{\alpha_i|i\neq j,\ k\}$ 的元素线性表出。把上面这种"用β替换α"的过程继续做下去，在第 p 步替换完之后，我们得到由p个β_i：

$$\beta_m,\ \beta_{m-1},\ \cdots,\ \beta_{m-p+1}$$

和没被替换掉的 $n-p$个α_i 所组成的子集，并且此子集中的全部n个元素生成模M。

这样，假如 $n<m$，，那么做完第 n 步替换之后将得到 n 个 β_i：

$$\beta_m,\ \beta_{m-1},\ \cdots,\ \beta_{m-n+1}\ ,$$

而且是M的一组生成元。由于 $m-n+1\geqslant 2$，从而 β_1 将被 β_m，β_{m-1}，…，β_{m-n+1} 线性表出。这与β_1，β_2，…，β_m 是 M的基底相矛盾。因此必然有$m\leqslant n$。同理可以推得$n\leqslant m$。故而$m=n$。

有了除环 R 的"维数不变性"，就能给出除环 R上自由模ની数量特征，即有

除环 R 上的两个自由模 M 与 M' 是同构的充分必要条件是 $rankM=rankM'$。

习　题

1. 设R为任意有恒等元素的环，e_1，e_2，…，e_n 是自由模 $R^{(n)}$ 的一个基底。令f_1，f_2，…，f_m为$R^{(n)}$ 中之任意 m个元素：

$$f_i=\sum_{j=1}^{n}a_{ij}e_j,\ A=(a_{ij})$$

证明：$f_1,f_2,\cdots,f_m$是$R^{(n)}$ 的一个基底$\Longleftrightarrow$存在$n\times m$矩阵B，使得

$$BA=I_n,\ AB=I_m.$$

从而证明：$R^{(m)} \simeq R^{(n)} \Longleftrightarrow$ 存在$A_{m\times n}$与$B_{n\times m}$，使得

$$BA=I_n,\ AB=I_m.$$

2．设 R为有恒等元素的可换环．M 与 N都是R上的模．对任意一个模同态$\eta\in Hom(M, N)$，按以下规则定义倍数运算：

$$(k\eta)\alpha=k(\eta(\alpha)),\ k\in R,\ \alpha\in M.$$

证明：$Hom(M, N)$ ）做成R上的模．进而证明：

$$rank Hom(R^{(m)}, R^{(n)})=mn.$$

3．求$Z^{(3)}$的子模$LC(f_1, f_2, f_3)$的一个基底．其中

$$f_1=(1, 0, 0),$$
$$f_2=(2, -1, 0),$$
$$f_3=(0, 3, 1).$$

4．求（$\mathbf{Q}[\lambda]$）$^{(3)}$的子模$LC(f_1, f_2, f_3)$的一个基底，其中$\mathbf{Q}$为有理数域，而

$$f_1=(2\lambda-1, \lambda, \lambda^2+3),$$
$$f_2=(\lambda, \lambda, \lambda^2),$$
$$f_3=(\lambda+1, 2\lambda, 2\lambda^2-3).$$

5．求由一切满足条件

$$x_1+2x_2+3x_3=0,$$
$$x_1+4x_2+9x_3=0,$$

的(x_1, x_2, x_3)所组成的$Z^{(3)}$的子模的一个基底．

6．证明：任一循环群M做为Z—模是自由的 $\Longleftrightarrow$ M是无限循环群．

7．设R为除环．证明：R上的两个自由模 M与M'是同构的$\Longleftrightarrow rankM=rankM'$．

8．设M为除环R上的模．$\alpha_1, \alpha_2, \cdots, \alpha_s\in M$．证明：

（1）$\alpha_1,\alpha_2,\cdots,\alpha_s$是线性相关的$\Longleftrightarrow$存在某一个$\alpha_k$，它是前面一些$\alpha_i$ $(1\leqslant i<k)$ 的线性组合．

（2）如果$\alpha_1,\alpha_2,\alpha_3$是线性无关的，那么

$$\alpha_1+\alpha_2,\ \alpha_2+\alpha_3,\ \alpha_3+\alpha_1$$

是线性无关的$\Longleftrightarrow R$的特征数不等于2.

9. 设R为有恒等元素的环，并具有"维数不变性". 证明：如果M_1与M_2均为R上的自由模. 那么$M_1 \oplus M_2$也是R上的自由模，并且

$$rank\ (M_1 \oplus M_2) = rankM_1 + rankM_2.$$

10. 设R为有恒等元素的环，并且没有零因子. 证明：如果对任意的$r, s \in R$均存在不同时为零的元素$a, b \in R$，使得$ar + bs = 0$，那么R具有"维数不变性".

11. 设K是有恒等元素的环，N是K上的模，N中存在可数无穷多个元素：

$$e_1, e_2, \cdots, e_m, \cdots \qquad (1)$$

使得N中每一个元素均能用（1）中有限个元素线性表示出来，并且这种表示法恒唯一. 令

$$R = Hom_k\ (N, N).$$

试证：把R做为R—模来看时，对任意一个正整数n，其中均有n个元素组成一个基底.

§3 自由模的子模与同态映射

我们先来考察自由模的子模。在上一章的讨论过程中已经知道，循环模的子模未必是循环模；一般地，有限生成模的子模未必是有限生成模。进而，我们自然想到：自由模的子模是否还是自由模？

以下两个例子具体的回答了这个问题。

首先，令R为剩余类环Z_6，即

$$R=\{\overline{0},\overline{1},\overline{2},\overline{3},\overline{4},\overline{5}\}=Z_6;$$

再取M为加法群$\{Z_6;+\}$。这样，M就自然成为一个R—模，而且是秩数等于1的自由模：

$$M=[\overline{1}],\ rankM=1.$$

于是，模M的子集$N=\{\overline{0},\overline{3}\}$是一个子模，显然，$N$不是$M$的自由子模。

此处环$R=Z_6$，这是一个交换环（当然有恒等元素），但是有真零因子。

其次再看一个例子。设$R=Z[\lambda]$，即R是整数环Z上的一个未定元λ的多项式环。显然，这个环R是交换环（当然有恒等元素），而且没有真零因子。这说明$R=Z[\lambda]$是一个较强的环。

现在还是把R本身看做R—模。则有

$$R=[1],$$

即R做为R—模是自由的，并且$rankR=1$。

令

$$N=LC(2,\lambda)$$

即N是由2与λ这两个元素生成的子模。我们考察这个子模N是否为自由子模。

首先，N不是零秩的。

其次，这个N也是环$Z[\lambda]$的理想子环，但不是主理想子环，即它不能由一个元素来生成。这表明，N做为子模不是1秩的。

再次，可以指出N中任意的两个元素：

$$f_1(\lambda)\ ,\ f_2(\lambda)\ \in N,$$

关于环$Z[\lambda]$都是线性相关的。事实上，不难找到环$Z[\lambda]$中的两个元素：

$$k_1=f_2(\lambda)\ ,\ k_2=-f_1(\lambda)\ ,$$

以这两个元素做系数，便有

$$k_1f_1(\lambda)+k_2f_2(\lambda)=0.$$

这就断定$f_1(\lambda)$，$f_2(\lambda)$在$Z[\lambda]$上是线性相关的。进而，自然可知：N中任意多于两个的元素关于环$Z[\lambda]$也总是线性相关的。

总而言之，N中任意一组元素都不能做成基底。故而，N不是自由模。

但是，对于条件更强一些的环R，我们可以证明，R上自由模之子模亦为自由模。即有

定理 1 设D为主理想环，那么，D上自由模M的子模N也是自由模，并且

$$rankN\leqslant rankM.$$

证 设$rankM=n$，且$n>0$。于是，不妨认为$M=D^{(n)}$。对秩数n做数学归纳法。

当$n=1$时，$M=D^{(1)}=D$。于是，M的子模N就是D的理想子环。因为D是主理想环，所以N是一个主理想子环，即有$f\in N$，使

$$N=(f)\ ,$$

此处符号(f)表示$N=(f)$是由元素f生成的理想子环。

这样，当$f=0$时，N是零秩自由模；而当$f\neq 0$时，因为D是主理想环，所以D没有真零因子。从而，可知

$$kf = 0 \Longrightarrow k = 0 .$$

这就说明$N = (f) = [f]$，即N是1秩自由模．由此，定理对$n = 1$的情形成立．

归纳假设定理对$n-1$的情形已成立，下面看秩数等于n的模的情形．取$D^{(n)}$的一个基底：

$$e_1, \ e_2, \ \cdots, \ e_n;$$

令

$$D^{(n-1)} = [e_2, \ \cdots, \ e_n],$$

这是一个$n-1$秩的自由模．于是，有商模

$$D^{(n)} \Big/ D^{(n-1)} = LC(\overline{e_1}) = [\overline{e_1}],$$

即 $rank\, D^{(n)} \Big/ D^{(n-1)} = 1$，其中$\overline{e}_1 = e_1 + D^{(n-1)}$．

从而有

$$\overline{N} = (N + D^{(n-1)}) \Big/ D^{(n-1)}$$

是商模 $D^{(n)} \Big/ D^{(n-1)}$的一个子模．如果$\overline{N} = \{\overline{0}\}$，那么$N \subseteq D^{(n-1)}$．由归纳假设，可知定理成立．下面考察$\overline{N} \neq \{\overline{0}\}$的情形．分两种情况：

（1）$N \cap D^{(n-1)} \neq \{0\}$

这时，$\overline{N}$做为1秩自由模$\overline{D^{(n)}} = D^{(n)} \Big/ D^{(n-1)}$的子模，我们已知它也是自由的，且因$\overline{N} \neq \{\overline{0}\}$，故而$\overline{N}$是1秩的．即有

$$\overline{N} = [\overline{f_1}],$$

其中 $\overline{f_1} = f_1 + D^{(n-1)}$．由于$\overline{N} = (N + D^{(n-1)}) \Big/ D^{(n-1)}$，我们可以取成 $f_1 \in N$．

再由 $N \cap D^{(n-1)}$ 是 $D^{(n-1)}$ 的子模，依归纳假设可知$N \cap D^{(n-1)}$是自由模，可令

$$N\cap D^{(n-1)}=[f_2,\ \cdots,f_m],$$

且有$m-1\leqslant n-1$。现在我们可以证明 f_1，f_2，…，f_m 恰好是子模N的一个基底。为此先证它是N的一组生成元素。设y为N中任一元素，于是，$\bar{y}\in\bar{N}$。故有

$$\bar{y}=b_1\bar{f}_1,\ b_1\in D$$

从而可知

$$y-b_1f_1\in D^{(n-1)}.$$

又因 f_1 取在N里，则有 $y-b_1f_1\in N$。这样就有

$$y-b_1f_1\in N\cap D^{(n-1)}.$$

因而 $y-b_1f_1$ 能用$N\cap D^{(n-1)}$ 的基底f_2，…，f_m线性表出：

$$y-b_1f_1=b_2f_2+\cdots+b_mf_m.$$

b_2，…，$b_m\in D$。即有

$$y=b_1f_1+b_2f_2+\cdots+b_mf_m,$$

故而 f_1，f_2，…，f_m是N的一组生成元素。

其次，指出 f_1，f_2，…，f_m关于D是线性无关的。若有

$$b_1f_1+b_2f_2+\cdots+b_mf_m=0,$$

那么

$$b_1\bar{f}_1=-(b_2\bar{f}_2+\cdots+b_m\bar{f}_m)=\bar{0}.$$

因为$\bar{f}_1$是$\bar{N}$的基底，所以$b_1=0$。于是有

$$b_2f_2+\cdots+b_mf_m=0.$$

而f_2，…，f_m是$N\cap D^{(n-1)}$的基底，故得

$$b_2=0,\ \cdots,\ b_m=0.$$

这就得出f_1，f_2，…，f_m在D上是线性无关的。即得f_1，f_2，…，f_m是子模N的基底，且有$m\leqslant n$。

（2）$N\cap D^{(n-1)}=\{0\}$

这时对N中任一元素y，有$\bar{y}=b_1\bar{f}_1$。从而

$$y-b_1f_1\in D^{(n-1)}.$$

又由 $y-b_1f_1\in N$，故而$y-b_1f_1\in N\cap D^{(n-1)}$。故而

$$y-b_1f_1=0\text{，即 }y=b_1f_1.$$

这就说明，f_1是N的生成元．而f_1显然关于D是线性无关的．即得f_1是子模N的基底．

这就证明了$\overline{N}\neq\{\overline{0}\}$时定理成立．到此，定理1，被完全证明了．▮

推论 域F上的有限维线性空间V的子空间W也是有限维的，并且$dimW\leqslant dimV$．特别地，$W=V\Longleftrightarrow dim\ W=dimV$．▮

再有一点可以提出的，就是推论中的后一个结论对一般的自由模来说是否也成立？请读者考虑．

下面讨论自由模的同态映射．在这里充分显示出矩阵的重要作用和意义．

设R为任一有恒等元素的环．M与M'均为R上的自由模．M有n个元素

$$\alpha_1,\ \alpha_2,\ \cdots,\ \alpha_n$$

做成的基底；M'有m个元素

$$\alpha_1',\ \alpha_2',\ \cdots,\ \alpha_m'$$

做成的基底．令$\sigma\in Hom\ (M,\ M')$，即σ是从M到M'的一个模同态映射．于是α_1，α_2，…，α_n在σ之下的象是模M'中的n个元素，从而它们都能用M'的基底α_1'，α_2'，…，α_m'以唯一的形式线性表示出来：

$$\begin{cases}\sigma(\alpha_1)=a_{11}\alpha_1'+a_{12}\alpha_2'+\cdots+a_{1m}\alpha_m',\\ \sigma(\alpha_2)=a_{21}\alpha_1'+a_{22}\alpha_2'+\cdots+a_{2m}\alpha_m',\\ \qquad\vdots\\ \sigma(\alpha_n)=a_{n1}\alpha_1'+a_{n2}\alpha_2'+\cdots+a_{nm}\alpha_m'.\end{cases}\tag{1}$$

其中$a_{ij}\in R$；$i=1,\ 2,\ \cdots,n$，$j=1,2,\cdots,m$．这样，由这$n\times m$个表示系数得到一个唯一确定的$n\times m$矩阵：

$$A=\begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1m} \\ a_{21} & a_{22} & \cdots & a_{2m} \\ \cdot & \cdot & \cdots & \cdot \\ a_{n1} & a_{n2} & \cdots & a_{nm} \end{pmatrix} \qquad (2)$$

称A为σ关于基底$\alpha_1, \alpha_2, \cdots, \alpha_n$与$\alpha'_1, \alpha'_2, \cdots, \alpha'_m$的表示矩阵。

反过来，如果事先给出了一个$n\times m$矩阵$A=(a_{ij})$如（2）。于是，由于一个模同态唯一的决定于它对基底中每一个元素的象，因此按照（1）式就能得到一个唯一确定的模同态：

$\sigma: M \longrightarrow M'$。

并且明显可见，这个模同态σ关于基底

$\alpha_1, \alpha_2, \cdots, \alpha_n$与$\alpha'_1, \alpha'_2, \cdots, \alpha'_m$

的表示矩阵恰好就是事先给出的$n\times m$矩阵$A=(a_{ij})$。

以上讨论表明，对于任意的两个自由R—模M与M'，它们之间的模同态映射σ与R上的矩阵$A=(a_{ij})$存在着自然的、重要的联系，用这种联系使得每一个模同态

$\sigma: M \longrightarrow M'$

都能用R上的一个矩阵$A=(a_{ij})$具体地表示出来。概括地说就是，自由模之间的模同态映射能够用R上的矩阵来刻划：

首先，在自由模M与M'中分别取定一个基底，如

$\alpha_1, \alpha_2, \cdots, \alpha_n$与$\alpha'_1, \alpha'_2, \cdots, \alpha'_m$。

其次，把模同态σ作用于基底$\alpha_1, \alpha_2, \cdots, \alpha_n$中各个元素上的象用基底$\alpha'_1, \alpha'_2, \cdots, \alpha'_m$线性表示出来，如前面的（1）式。

结论：规则

$\eta: \sigma \longmapsto A$,

是$Hom_R(M, M')$到$M_{n\times m}(R)$的一个双射（一一对应）。

特别地，当$M=M'$，并且把$\alpha_1, \alpha_2, \cdots, \alpha_n$与$\alpha'_1, \alpha'_2, \cdots, \alpha'_m$取成模$M$的同一个基底，即令

$n=m$ 且 $\alpha_1=\alpha'_1, \alpha_2=\alpha'_2, \cdots, \alpha_n=\alpha'_n$。

这时，前面的（1）式就是

$$\begin{cases}\sigma(\alpha_1)=a_{11}\alpha_1+a_{12}\alpha_2+\cdots+a_{1n}\alpha_n,\\ \sigma(\alpha_2)=a_{21}\alpha_1+a_{22}\alpha_2+\cdots+a_{2n}\alpha_n,\\ \qquad\vdots\\ \sigma(\alpha_n)=a_{n1}\alpha_1+a_{n2}\alpha_2+\cdots+a_{nn}\alpha_n.\end{cases}$$

而σ是自由模M的任一自同态，它关于基底

$$\alpha_1,\ \alpha_2,\ \cdots,\ \alpha_n$$

的表示矩阵$A=(a_{ij})$则是一个n阶方阵．即有

$$\eta:\sigma\longmapsto A$$

是从$Hom(M,\ M)$到$M_n(R)$的一个一一对应（双射）．

用矩阵刻划自由模的同态映射的重要意义和深刻性，远不止于使得Hom_R（M，M'）与$M_{n\times m}$（R）的成员之间能够一一对应起来．下面我们就来进一步揭示这种一一对应η更为本质的内涵．

我们已经知道，Hom_R（M，M'）关于模同态的加法做成加法群；而当R为交换环时，Hom（M，M'）还是R上的一个左模．相应地，$M_{n\times m}(R)$也是加法群、左模．特别地，当$M=M'$时，还有

$$\{Hom_R(M,\ M);\ +,\ \cdot\}$$

做成一个环——模M的全自同态环，其中的乘法是模同态映射的合成．自然相应地也有$M_n(R)$也是环——R上的n阶全阵环．

既然情况是这样，我们自然会问：一一对应η是否保持相关的运算？或者说，一一对应η是否使得相应的代数结构不变？

首先，我们不难肯定如下的结论，即

定理 2 设M与M'均为环R上的自由模．

令

$$M=[\alpha_1,\ \alpha_2,\ \cdots,\ \alpha_n],$$
$$M'=[\alpha_1',\ \alpha_2',\ \cdots,\ \alpha_m'].$$

那么一一对应

$$\eta: \sigma \longmapsto A, \ \forall \sigma \in Hom_R(M, M'),$$

其中A为σ关于基底$\alpha_1, \alpha_2, \cdots, \alpha_n$与$\alpha'_1, \alpha'_2, \cdots, \alpha'_m$的表示矩阵，是加法群的同构映射：

$$\eta: Hom(M, M') \longrightarrow M_{n\times m}(R),$$

如果R是交换环，η还是$Hom_R(M, M')$与$M_{n\times m}(R)$的一个R—模同构。

定理2的证明做为习题留给读者去完成。▮

较为细致而又多少有些复杂的是有关乘法的情况。对此，我们考虑环R上的三个自由模M，M'与M''。它们分别有基底：

$$\alpha_1, \alpha_2, \cdots, \alpha_n;$$
$$\alpha'_1, \alpha'_2, \cdots, \alpha'_m;$$
$$\alpha''_1, \alpha''_2, \cdots, \alpha''_S.$$

即有

$$M = [\alpha_1, \alpha_2, \cdots, \alpha_n],$$
$$M' = [\alpha'_1, \alpha'_2, \cdots, \alpha'_m],$$
$$M'' = [\alpha''_1, \alpha''_2, \cdots, \alpha''_S],$$

设σ是M到M'的任意一个模同态映射，关于基底$\alpha_1, \alpha_2, \cdots, \alpha_n$与$\alpha'_1, \alpha'_2, \cdots, \alpha'_m$的表示矩阵为$n\times m$矩阵$A=(a_{ij})$；$\tau$是$M'$到$M''$的任意一个模同态映射，关于基底$\alpha'_1, \alpha'_2, \cdots, \alpha'_m$与$\alpha''_1, \alpha''_2, \cdots, \alpha''_S$的表示矩阵为$m\times s$矩阵$B=(b_{jk})$。于是，$\sigma$与$\tau$的合成是$M$到$M''$的一个模同态映射$\tau\sigma$。我们来计算这个模同态$\tau\sigma$关于基底$\alpha_1, \alpha_2, \cdots, \alpha_n$与$\alpha''_1, \alpha''_2, \cdots, \alpha''_S$的表示矩阵等于什么。为此，按照模同态映射的表示矩阵的定义，这需要计算$\tau\sigma$作用基底$\{\alpha_1, \alpha_2, \cdots, \alpha_n\}$的各个元素的象被基底$\alpha''_1, \alpha''_2, \cdots, \alpha''_S$线性表出的诸系数。即有

$$\begin{aligned}\tau\sigma(\alpha_i) &= \tau(a_{i1}\alpha'_1 + a_{i2}\alpha'_2 + \cdots + a_{im}\alpha'_m) \\ &= a_{i1}(\tau\alpha'_1) + a_{i2}(\tau\alpha'_2) + \cdots + a_{im}(\tau\alpha'_m) \\ &= a_{i1}(b_{11}\alpha''_1 + b_{12}\alpha''_2 + \cdots + b_{1S}\alpha''_S) + \\ &\quad + a_{i2}(b_{21}\alpha''_1 + b_{22}\alpha''_2 + \cdots + b_{2S}\alpha''_S) +\end{aligned}$$

$$+\cdots+$$

$$+a_{im}(b_{m1}\alpha_1''+b_{m2}\alpha_2''+\cdots+b_{mS}\alpha_S'')$$

$$=(a_{i1}b_{11}+a_{i2}b_{21}+\cdots+a_{im}b_{m1})\alpha_1''+$$

$$+(a_{i1}b_{12}+a_{i2}b_{22}+\cdots+a_{im}b_{m2})\alpha_2''+$$

$$+\cdots+$$

$$+(a_{i1}b_{1S}+a_{i2}b_{2S}+\cdots+a_{im}b_{mS})\alpha_S'',$$

其中 $i=1, 2, \cdots, n$. 由此可知，$\tau\sigma$ 关于基底 $\alpha_1, \alpha_2, \cdots, \alpha_n$与$\alpha_1'', \alpha_2'', \cdots, \alpha_S''$的表示矩阵

$$C=(c_{ij}),\quad c_{ij}=a_{i1}b_{1j}+a_{i2}b_{2j}+\cdots+a_{im}b_{mj},$$

其中 $i=1, 2, \cdots, n; j=1, 2, \cdots, s$.因此，即有

$$C=AB.$$

特别地，当 σ，τ 都是自由模$M=[\alpha_1, \alpha_2, \cdots, \alpha_n]$ 的自同态，并且

$$\eta: \sigma \longmapsto A,$$
$$\tau \longmapsto B,$$

则有

$$\eta: \tau\sigma \longmapsto AB.$$

把以上的讨论归纳起来可以得到如下的结论。即有

定理 3 设M为环R上的自由模，任取M的一个基底$\alpha_1, \alpha_2, \cdots, \alpha_n$，那么映射

$$\eta: \sigma \longmapsto A,$$

其中A是自同态σ关于基底 $\alpha_1, \alpha_2, \cdots, \alpha_n$ 的表示矩阵，是环$Hom_R(M, M)$ 与$M_n(R)$ 的反同构映射。而当R为交换环时，映射

$$\eta': \sigma \longmapsto A'$$

则是环$Hom_R(M,M)$ 与$M_n(R)$ 的同构映射。▮

习　　题

1. 设R是主理想环，M是R上的有限生成模，有由n个元素组成的生成组。试证：M的每一个子模N也都是有限生成的，而且均可由m个元素生成，使$m\leqslant n$。

2. 设M_1，M_2都是主理想环R上的模。$r,p\in R$，其中p为素元。试证：

1）$rM_1=\{rx|x\in M_1\}$和$M_1[r]=\{x\in M_1|rx=0\}$都是M_1的子模。

2）$torM_1=\{x\in M_1|annx\neq 0\}$是$M_1$的子模。

3）$M_1[p]$是域$R/(p)$上的线性空间。

4）对于每一个正整数n，均有R—模同构：

$$\left(R/(p^n)\right)[p]\simeq R/(p),\quad p^m\left(R/(p^n)\right)\simeq R/(p^{n-m})$$

其中$0\leqslant m\leqslant n$。

5）如果R—模$M\simeq M_1+M_2$，那么

$rM\simeq rM_1+rM_2$，$M[r]\simeq M_1[r]+M_2[r]$。

6）如果有同构映射

$\varphi: M_1\longrightarrow M_2$，

那么

$\varphi: torM_1\longrightarrow torM_2$，

也是同构映射，并且

$\varphi: M_1[p]\longrightarrow M_2[p]$

也是同构映射。

3. 证明：如果R是有恒等元素的交换环，并且每一个自由R—模的每一个子模均是自由的，那么R是主理想环。

4. 设M是无零因子的交换环R上的自由模，试证：$torM=\{0\}$，反过来是否也对，为什么？

5．设M是主理想环R上的循环模，$M=Rx$，$\mathrm{ann}\,x=(r)$．则有

1）如果$s\in R$，$(s,r)=1$，那么$sM=M$，$M[s]=\{0\}$．

2）如果$s\setminus r$，令$sk=r$，那么$sM\simeq R/(k)$，$M[s]\simeq R/(s)$．

6．设M是主理想环R上的循环模，$M=Rx$，$\mathrm{ann}\,x=(r)$．则有

1）M的每一个子模N都是循环的，且若有$N=Ry$，$\mathrm{ann}\,y=(s)$．则有$s\setminus r$．

2）对于每一个包含(r)的理想(s)，M恰好有一个子模$N=Ry$，使$\mathrm{ann}\,y=(s)$．

§4 主理想环上有限生成模的结构

本节讨论有限生成模的结构问题，这里我们对 R是主理想环的情形，给出 R上有限生成模的分解定理和不变性定理两个方面的重要结果。虽然主理想环是比较特殊的环，但是主理想环上有限生成模的结构理论不仅具有完整性与深刻性的特点，同时还有许多方面的具体应用。

定理 1 设 R为主理想环，$M(\neq 0)$ 是R上的有限生成模，那么M可以表成循环模的直和：

$$M = Rz_1 \oplus Rz_2 \oplus \cdots \oplus Rz_s,$$

并使阶理想满足

$$\operatorname{ann} z_1 \supseteq \operatorname{ann} z_2 \supseteq \cdots \supseteq \operatorname{ann} z_s, \quad \operatorname{ann} z_k \neq R.$$

$k=1, 2, \cdots, s$.

证 先任取M的一个有限生成组$x_1, x_2, \cdots, x_n$，则有

$$M = Rx_1 + Rx_2 + \cdots + Rx_n.$$

这里的和未必是直和，更谈不到阶理想成递降序列。我们的想法是：把生成组$x_1, x_2, \cdots, x_n$换成另外的一个生成组$y_1, y_2, \cdots, y_n$，使循环子模 $Ry_1, Ry_2, \cdots, Ry_n$的和是直和，同时它们的阶理想成递降序列。

为此我们拿自由模$R^{(n)} = [e_1, e_2, \cdots, e_n]$ 与模M做比较。这时，自然有一个同态映射 η，使

$$R^{(n)} \overset{\eta}{\sim} M,$$

其中

$$\eta: a_1e_1 + a_2e_2 + \cdots + a_ne_n \longmapsto a_1x_1 + a_2x_2 + \cdots + a_nx_n$$

于是由模同态基本定理，则有

$$R^{(n)} / K \simeq M,$$

其中 $K=ker\eta$。根据上一节的定理 1，K 是自由模，因此可以令 $f_1, f_2, \cdots, f_m$ 为 K 的一个有限生成组。把每一个 f_i $(i=1, 2, \cdots, m)$ 用 $R^{(n)}$ 的基底 $e_1, e_2, \cdots, e_n$ 表示出来，即有

$$\begin{cases} f_1 = a_{11}e_1 + a_{12}e_2 + \cdots + a_{1n}e_n, \\ f_2 = a_{21}e_1 + a_{22}e_2 + \cdots + a_{2n}e_n, \\ \quad \vdots \\ f_m = a_{m1}e_1 + a_{m2}e_2 + \cdots + a_{mn}e_n, \end{cases}$$

则得表示系数做成的 $m\times n$ 矩阵 $A=(a_{ij})$。

这样，由第一节定理8，$A=(a_{ij})$ 相抵于一个标准形，即可取 m 阶可逆矩阵 $Q=(q_{ij})$ 及 n 阶可逆矩阵 $P=(p_{ij})$，使得

$$B=QAP^{-1}=\begin{pmatrix} d_1 & & & & & \\ & d_2 & & & & \\ & & \ddots & & & \\ & & & d_r & & \\ & & & & 0 & \\ & & & & & \ddots \\ & & & & & & 0 \end{pmatrix}$$

其中 $d_1, d_2, \cdots, d_r$ 均不为 0，而且依次能整除：

$$d_1 \diagdown d_2 \diagdown \cdots \diagdown d_r.$$

这样，以 P, Q 为过渡矩阵，可使基底 $e_1, e_2, \cdots, e_n$ 与生成组 $f_1, f_2, \cdots, f_m$ 分别换成新的基底与生成组如下：

$$\begin{pmatrix} e_1' \\ e_2' \\ \vdots \\ e_n' \end{pmatrix} = P\begin{pmatrix} e_1 \\ e_2 \\ \vdots \\ e_n \end{pmatrix}, \quad \begin{pmatrix} f_1' \\ f_2' \\ \vdots \\ f_m' \end{pmatrix} = Q\begin{pmatrix} f_1 \\ f_2 \\ \vdots \\ f_m \end{pmatrix}.$$

从而使新生成组 $f_1', f_2', \cdots, f_m'$ 用新基底 $e_1', e_2', \cdots, e_n'$ 线性表出的系数矩阵恰好就是上面的对角阵：

$$B=diag\{d_1, d_2, \cdots, d_r, 0, \cdots, 0\}$$

即

$$\begin{pmatrix} f_1' \\ f_2' \\ \vdots \\ f_m' \end{pmatrix} = B \begin{pmatrix} e_1' \\ e_2' \\ \vdots \\ e_n' \end{pmatrix}$$

写成单个的式子就是

$$\begin{aligned} f_1' &= d_1 e_1', \\ f_2' &= d_2 e_2', \\ &\vdots \\ f_r' &= d_r e_r', \\ f_{r+1}' &= 0, \\ &\vdots \\ f_m' &= 0. \end{aligned}$$

与上述更换基底和生成组的过程相对应，令

$$\begin{pmatrix} y_1 \\ y_2 \\ \vdots \\ y_n \end{pmatrix} = P \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix},$$

则使模 M 的原生成组 $x_1, x_2, \cdots, x_n$ 换成了新生成组 $y_1, y_2, \cdots, y_n$。

又由于

$$\eta: e_i \longmapsto x_i, \quad i = 1, 2 \cdots, n,$$

而

$$e_i' = p_{i1} e_1 + p_{i2} e_2 + \cdots + p_{in} e_n, \quad i = 1, 2, \cdots, n,$$

于是

$$\begin{aligned} \eta(e_i') &= \eta(p_{i1} e_1 + p_{i2} e_2 + \cdots + p_{in} e_n) \\ &= p_{i1}\eta(e_1) + p_{i2}\eta(e_2) + \cdots + p_{in}\eta(e_n) \\ &= p_{i1} x_1 + p_{i2} x_2 + \cdots + p_{in} x_n \\ &= y_i. \end{aligned}$$

这就是

$$\eta: e_i' \longmapsto y_i, \quad i=1, 2, \cdots, n.$$

下一步便可指出，M的这个新生成组y_1，y_2，…，y_n即合所求。

首先指出，和式$M=Ry_1+Ry_2+\cdots+Ry_n$是直和。为此，若有

$$b_1y_1+b_2y_2+\cdots+b_ny_n=0, \quad b_i\in R,$$

从而可知$b_1y_1+b_2y_2+\cdots+b_ny_n$在同态映射$\eta$之下的原象

$$b_1e_1'+b_2e_2'+\cdots+b_ne_n'\in K.$$

于是

$$\begin{aligned}b_1e_1'+b_2e_2'+\cdots+b_ne_n' &= c_1f_1'+c_2f_2'+\cdots+c_rf_r' \\ &= c_1d_1e_1'+c_2d_2e_2'+\cdots+c_rd_re_r'.\end{aligned}$$

因为e_1'，e_2'，…，e_n'是基底，故而必有

$$b_1=c_1d_1, \ b_2=c_2d_2, \ \cdots, \ b_r=c_rd_r, \ b_{r+1}=0, \ \cdots,$$

$b_n=0$。

由于 $d_ie_i'=f_i'\in K$，所以 $\eta(d_ie_i')=d_iy_i=0$，$i=1, 2, \cdots, r$。则有

$$\begin{aligned}&b_1y_1=c_1d_1y_1=0, \\ &b_2y_2=c_2d_2y_2=0, \\ &\quad\vdots \\ &b_ry_r=c_rd_ry_r=0, \\ &b_{r+1}y_{r+1}=0, \ \cdots, \ b_ny_n=0.\end{aligned}$$

这就得出

$$M=Ry_1+Ry_2+\cdots+Ry_n=Ry_1\oplus Ry_2\oplus\cdots\oplus Ry_n.$$

其次指出，y_1，y_2，…，y_r，y_{r+1}，…，y_n的阶理想成递降序列。

先考察前r个元素y_1，y_2，…，y_r的阶理想。由于$d_iy_i=0 \Longrightarrow (d_i)\subseteq ann\,y_i$。反之，若$ay_i=0$，则有

$$ae_i' \in K \Longrightarrow ae_i' = u_1 f_1' + u_2 f_2' + \cdots + u_r f_r'$$
$$= u_1 d_1 e_1' + u_2 d_2 e_2' + \cdots + u_r d_r e_r',$$

可得

$$a = u_i d_i, \quad a \in (d_i)$$

故有$ann y_i \subseteq (d_i)$ 因此得到

$$ann y_1 = (d_1), \quad ann y_2 = (d_2), \quad \cdots, \quad ann y_r = (d_r).$$

再考察后$n-r$个元素y_{r+1}，…，y的阶理想。

若 $ay_i = 0$，$i = r+1$，…，n. 则有

$$ae_i' \in K, \quad 即 ae_i' = v_1 f_1' + v_2 f_2' + \cdots + v_r f_r'.$$

由 $i \geqslant r+1$，便知$a = 0$，即

$$ann y_i = 0, \quad i = r+1, \cdots, n.$$

总括以上所述，可得

$$M = Ry_1 \oplus Ry_2 \oplus \cdots \oplus Ry_n,$$

且有

$$ann y_1 \supseteq ann y_2 \supseteq \cdots \supseteq ann y_r \supseteq ann y_{r+1} \supseteq \cdots \supseteq ann y_n.$$

在y_i的阶理想$ann y_i$中可能有某些等于R,这相当于$Ry_i = 0$. 因此在直和式中可以把这样的加项去掉。令

$$ann y_1 = ann y_2 = \cdots = ann y_t = R, \quad ann y_{t+1} \neq R,$$

且令

$$z_1 = y_{t+1}, \quad z_2 = y_{t+2}, \quad \cdots, \quad z_S = y_n,$$

其中 $s = n - t$. 于是就有

$$M = Rz_1 \oplus Rz_2 \oplus \cdots \oplus Rz_S,$$

并且使得

$$ann z_1 \supseteq ann z_2 \supseteq \cdots \supseteq ann z_S, \quad ann z_k \neq R.$$

$k = 1, 2, \cdots, s$. 到此定理 1 被证明了. ▌

我们把定理 1 中关于有限生成模M的直和分解式叫做 M的**标准分解式**.

为了进一步讨论M的标准分解式的唯一性问题，我们把它的直和项分为两类. $ann z_i \neq 0$ 的集中在一起予以统一考虑；余者，

即 $\operatorname{ann} z_i = 0$ 的归为一类一并处理.

设 $\operatorname{ann} z_1 \neq 0$，…，$\operatorname{ann} z_r \neq 0$，$\operatorname{ann} z_{r+1} = 0$，…．$\operatorname{ann} z_s = 0$．令

$$\operatorname{tor} M = \{y \in M \mid \text{存在} a \neq 0 \text{ 使} ay = 0\}.$$

换句话说，$y \in \operatorname{tor} M \Longleftrightarrow \operatorname{ann} y \neq 0$．

命题 1

（1）$\operatorname{tor} M$ 是 M 的子模．

（2）$\operatorname{tor} M = Rz_1 \oplus Rz_2 \oplus \cdots \oplus Rz_r$．

证　先证明（1）成立．任取 y_1，$y_2 \in \operatorname{tor} M$，于是存在 $a_1 \neq 0$，$a_2 \neq 0$，使 $a_1 y_1 = 0$，$a_2 y_2 = 0$，则有

$$\begin{aligned} a_1 a_2 (y_1 - y_2) &= (a_1 a_2) y_1 - (a_1 a_2) y_2 \\ &= a_2 (a_1 y_1) - a_1 (a_2 y_2) \\ &= 0, \end{aligned}$$

而且 $a_1 a_2 \neq 0$．从而 $y_1 - y_2 \in \operatorname{tor} M$．

任取 $y \in \operatorname{tor} M$，有 $a \in R$，$a \neq 0$ 使 $ay = 0$．于是，对于任意的 $k \in R$，可得

$$a(ky) = (ak)y = (ka)y = k(ay) = 0,$$

从而 $ky \in \operatorname{tor} M$．这样，$\operatorname{tor} M$ 是模 M 的子模．

其次证明（2）成立．一方面不难看出：

$$Rz_1 \oplus Rz_2 \oplus \cdots \oplus Rz_r \subseteq \operatorname{tor} M.$$

另一方面，任取 $y = a_1 z_1 + a_2 z_2 + \cdots + a_s z_s \in M$，若有 $y \in \operatorname{tor} M$，则存在 $b \in R$，$b \neq 0$ 使 $by = 0$．即

$$b a_1 z_1 + b a_2 z_2 + \cdots + b a_s z_s = 0.$$

这时由定理 1 的证明过程我们知道，必有

$$b a_i z_i = 0, \quad i = 1, 2, \cdots, s,$$

而当 $i > r$ 时，又必有

$$b a_i = 0 \Longrightarrow a_i = 0.$$

于是，只能有

$$y = a_1 z_1 + a_2 z_2 + \cdots + a_r z_r.$$

故而 $y\in Rz_1\oplus Rz_2\oplus\cdots\oplus Rz_r$，$torM\subseteq Rz_1\oplus Rz_2\oplus\cdots\oplus Rz_r$。因而得到

$$torM=Rz_1\oplus Rz_2\oplus\cdots\oplus Rz_r.$$

命题1证明完了。▌

由命题1可知，交换环上的模M当中恒存在一个确定的子模$torM$，称$torM$为M的扭子模。若有$torM=M$，就说模M是扭模。明显可见，一个交换群G做为整数环Z上的模来看时，它的扭子模$torG$就是G中一切有限阶（周期）元素做成的子群。特别地，当$torG=G$时，G就是通常所说的周期群。

定理 2 主理想环R上的有限生成模M是它的扭子模与一个自由子模的直和。

证 由定理1，M有标准分解式：

$$M=Rz_1\oplus\cdots\oplus Rz_r\oplus Rz_{r+1}\oplus\cdots\oplus Rz_S,$$

其中

$$annz_1\supseteq\cdots\supseteq annz_r\neq 0,$$

$$annz_{r+1}=0,\ \cdots,\ annz_S=0.$$

于是，由命题1则有

$$torM=Rz_1\oplus\cdots\oplus Rz_r,$$

从而

$$M=torM\oplus(Rz_{r+1}\oplus\cdots\oplus Rz_S).$$

容易指出$Rz_{r+1}\oplus\cdots\oplus Rz_S$是$M$的一个自由子模，这是因为，如果

$$a_{r+1}z_{r+1}+\cdots+a_Sz_S=0$$

则必有

$$a_iz_i=0,\ i=r+1,\ \cdots,\ s.$$

并且必有

$$a_{r+1}=0,\ \cdots,\ a_S=0.$$

即$Rz_{r+1}\oplus\cdots\oplus Rz_S$是$M$的一个自由子模.这样就证明了定理2.▌

定理2的意思是说，主理想环R上的有限生成模M均由两种

类型的子模“合并”而成。当中一个成份是M的一个唯一确定的子模$torM$,另外一个成份则是M的某一个自由子模。自由子模的结构是简单的，也是清楚的。而扭子模$torM$虽然是由M唯一决定的，但是它的结构并不象自由模那样简单，我们还没有完全弄清楚它的结构。因此，我们下面主要的目标是研究扭模的结构。为此进一步分解它的直和项。

首先，我们给出如下的一个基本事实。

命题 2

（1）若$M=Rx$, $annx=(d)$, $d=gh$, $(g,h)=1$. 则有
$M=Ry\oplus Rz$; $anny=(g)$, $annz=(h)$.

（2）若$M=Ry\oplus Rz$, $anny=(g)$, $annz=(h)$, $(g,h)=1$. 则有

$$M=Rx,\ annx=(gh).$$

证 先证（1）成立。令 $y=hx$, $z=gx$. 于是取a, $b\in R$, 使 $ah+bg=1$. 则有

$$x=(ah+bg)x=ahx+bgx=ay+bz\in Ry+Rz.$$

从而 $M=Ry+Rz$.

进而，若 $u\in Ry\cap Rz$, 则有$u=c_1y$, $u=c_2z$. 从而

$$gu=g(c_1y)=(gc_1)y=(c,g)y=c_1(gy)=c_1(g(hx))=c_1(gh)x=0;$$
$$hu=h(c_2z)=c_2hgx=0.$$

于是

$$u=1\cdot u=(ah+bg)u=ahu+bgu=0.$$

故而$M=Ry\oplus Rz$.

并且由于

$$gy=g(hx)=(gh)x=dx=0,$$

而对任意的 a, 有

$$ay=0\Longrightarrow ahx=0.$$

这样，由 x 的阶理想 $(d)=(gh)$, 则有

$$gh\setminus ah\Longrightarrow g\setminus a.$$

由此可得 $\operatorname{ann}y=(g)$。同理可得 $\operatorname{ann}z=(h)$.

再证（2）成立．由 $M=Ry\oplus Rz$，令 $x=y+z$，以及 $ah+bg=1$，于是

$$y=(ah+bg)y=ahy=ahy+ahz=ah(y+z)=ahx,$$

即 $y\in Rx$．而 $z=x-y\in Rx$，因此 $M\subseteq Rx$．故得 $M=Rx$．

为了指出 $\operatorname{ann}x=(gh)$，我们有

$$cx=0\Longrightarrow cy+cz=0\Longrightarrow cy=0,\ cz=0.$$

因而 $g\diagdown c$，$h\diagdown c$，由 $(g,h)=1$，可知 $gh\diagdown c$．即 $c\in(gh)$．并且还有 $(gh)x=gh(y+z)=ghy+ghz=0$．故得$\operatorname{ann}x=(gh)$．命题 2 证明完了．▌

在命题 2 的基础上，我们有以下重要的

定理 3 若$M=Rx$，$\operatorname{ann}x=(d)$，d有标准分解式：

$$d=p_1^{e_1}p_2^{e_2}\cdots p_t^{e_t}.$$

那么

$$M=Rx_1\oplus Rx_2\oplus\cdots\oplus Rx_t,$$

其中 $\operatorname{ann}x_i=(p_i^{e_i})$，$i=1, 2, \cdots, t$．

证 对 t 用数学归纳法．

当 $t=2$ 时，$d=p_1^{e_1}p_2^{e_2}$，而 $(p_1^{e_1}, p_2^{e_2})=1$．于是由命题2之（1）可知

$$M=Rx_1\oplus Rx_2,$$

其中 $\operatorname{ann}x_1=(p_1^{e_1})$，$\operatorname{ann}x_2=(p_2^{e_2})$．即 $t=2$时定理3成立．归纳假设对 $t-1$ 的情形定理 3 成立，下面看对 t 的情形．

事实上，由于 $d=p_1^{e_1}p_2^{e_2}\cdots p_t^{e_t}=(p_1^{e_1}\cdots p_{t-1}^{e_{t-1}})p_t^{e_t}$，而有

$$(p_1^{e_1}\cdots p_{t-1}^{e_{t-1}},\ p_t^{e_t})=1,$$

再据命题2之（1），可有

$$M=Ry+Rx_t,$$

其中$\operatorname{ann}y=(p_1^{e_1}\cdots p_{t-1}^{e_{t-1}})$，$\operatorname{ann}x_t=(p_t^{e_t})$

根据归纳法假设，则有

$$Ry = Rx_1 \oplus \cdots \oplus Rx_{t-1}$$

其中 $annx_i = (p_i^{e_i})$ ，$i = 1, 2, \cdots, t-1$。

于是便得

$$M = Rx_1 \oplus \cdots \oplus Rx_{t-1} \oplus Rx_t,$$

其中 $annx_i = (p_i^{e_i})$ ，$i = 1, 2, \cdots, t$。▉

如果循环模$M = Rx$，其生成元素 x 的阶理想是由一个素元的幂生成的，即$annx = (p^e)$，p为R中之素元素，则称 Rx 为**准素的**（循环模）。用此术语，定理 3 说明：任一循环扭模M均可分解成一些准素循环模的直和。由扭模的定义和定理 3 直接得出

定理 4 主理想环上的有限生成的扭模是准素的循环模的直和。▉

到此，对于主理想环 R上的有限生成的扭模M已经得出两种形式的直和分解，即

$$M = Rz_1 \oplus Rz_2 \oplus \cdots \oplus Rz_r,$$

其中生成元素的阶理想成递降序列：

$$annz_1 \supseteq annz_2 \supseteq \cdots \supseteq annz_r \neq 0。$$

若令 $annz_i = (d_i)$，则有 $d_1, d_2, \cdots, d_r$是依次能整除的：$d_1 \diagdown d_2 \diagdown \cdots \diagdown d_r$。

另外一种直和分解式就是

$$\begin{aligned} M = & Rx_{11} \oplus Rx_{12} \oplus \cdots \oplus Rx_{1l_1} \oplus \\ & \oplus Rx_{21} \oplus Rx_{22} \oplus \cdots Rx_{2l_2} \oplus \\ & \cdots \quad \cdots \quad \cdots \\ & \oplus Rx_{r1} \oplus Rx_{r2} \oplus \cdots \oplus Rx_{rl_r} \end{aligned}$$

其中Rx_{ij}都是准素的。即

$$annx_{ij} = (p_j^{e_{ij}}); \quad 1 \leqslant i \leqslant r, \quad 1 \leqslant j \leqslant l_i.$$

由命题 2 可知，扭模M的这两种形式的分解能够互相唯一的确定

出来。

例如，我们把有限交换群M做为 Z—模来考虑。令

$$M=Zu_1\oplus Zu_2\oplus Zu_3\oplus Zv_1\oplus Zv_2\oplus Zw_1\oplus Zw_2,$$

其中

$$annu_1=(3^2)，annu_2=(3^3)，annu_3=(3^4)，$$

$$annv_1=(5^2)，annv_2=(5^4)，$$

$$annw_1=(7)，annw_2=(7^3)．$$

这样，M就是一个阶为$3^9 5^6 7^4$的有限交换群，而直和分解式

$$M=Zu_1\oplus Zu_2+Zu_3\oplus Zv_1\oplus Zv_2\oplus Zw_1\oplus Zw_2$$

就是把M表成以准素循环模为直和项的分解。

另一方面，按命题 2 之（2），则有，

$$M=Zx_1\oplus Zx_2\oplus Zx_3,$$

其中

$$x_1=u_1,$$

$$x_2=u_2+v_1+w_1,$$

$$x_3=n_3+v_2+w_2,$$

并有

$$annx_1=(3^2)，$$

$$annx_2=(3^3\cdot 5^2\cdot 7)，$$

$$annx_3=(3^4\cdot 5^4\cdot 7^3)，$$

从而

$$annx_1\supseteq annx_2\supseteq annx_3,$$

或者是

$$3^2\diagdown 3^3\cdot 5^2\cdot 7\diagdown 3^4\cdot 5^4\cdot 7^3$$

显然，如果先有分解式

$$M=Zx_1\oplus Zx_2\oplus Zx_3,$$

使得

$$annx_1=(3^2)\supseteq annx_2=(3^3\cdot 5^2\cdot 7)\supseteq annx_3=(3^4\cdot 5^4\cdot 7^3)．$$

于是按命题 2 之（1），则有把M表成以准素循环模为项的直和分

解式：

$$M = Zu_1 \oplus Zu_2 \oplus Zu_3 \oplus Zv_1 \oplus Zv_2 \oplus Zw_1 \oplus Zw_2,$$

使得

$$ann\,u_1 = (3^2),\ ann\,u_2 = (3^3),\ ann\,u_3 = (3^4),$$
$$ann\,v_1 = (5^2),\ ann\,v_2 = (5^4),$$
$$ann\,w_1(7),\ ann\,w_2(7^3).$$

为了说话方便，我们把阶理想为 $ann\,x = (p^e)$ 的准素循环模 Rx简称为 p 型的。于是，下一步我们将这样来考虑：把扭模M的以准素循环模为项的直和分解式中属于同一 p 型的项集中起来予以统一研究。为此令

$$M_p = \{y \in M \mid \text{有正整数}k,\ \text{使}p^k y = 0\}.$$

换句话说，$y \in M_p \Longleftrightarrow Ry$是 p 型的。称M_p为M的一个**p—分支**。

命题 3

（1）M_p是M的子模，

（2）若 $p_1, p_2, \cdots, p_t$为R中不同的素元素，那么

$$M_{p_1} + M_{p_2} + \cdots + M_{p_t} = M_{p_1} \oplus M_{p_2} \oplus \cdots \oplus M_{p_t}.$$

换句话说，由不同的素元素所确定的分支，它们的和必为直和。

证 先证（1）成立。任取 $y_1, y_2 \in M_p$。则有正整数k_1，k_2使得

$$p^{k_1} y_1 = 0,\ p^{k_2} y_2 = 0.$$

从而

$$\begin{aligned} p^{k_1+k_2}(y_1 - y_2) &= p^{k_1+k_2} y_1 - p^{k_1+k_2} y_2 \\ &= p^{k_2}(p^{k_1} y_1) - p^{k_1}(p^{k_2} y_2) \\ &= 0. \end{aligned}$$

显然 $k_1 + k_2$ 是正整数，故有 $y_1 - y_2 \in M_p$。

又任取 $y \in M_p$，有正整数 k，使$p^k y = 0$。于是对任意的$a \in R$，则有

$$p^k(ay) = (p^k a)y = (ap^k)y = a(p^k y) = a \cdot 0 = 0.$$

这样就证明了M_p是M的一个子模。

再证（2）成立。为此令

$$y \in M_{p_i} \cap M_{p_1} + \cdots + M_{p_{i-1}} + M_{p_{i+1}} + \cdots + M_{p_t},$$

那么

$$y = y_i = y_1 + \cdots + y_{i-1} + y_{i+1} + \cdots + y_t,$$

其中 $y_i \in M_{p_i}$。于是对每一个 y_j（$j=1, 2, \cdots, t$）都有相应的正整数k_j，使得

$$p_j^{k_j} y_j = 0.$$

这样就有

$$p_i^{k_i} y = p_i^{k_i} y_i = 0;$$

$$p_1^{k_1} \cdots p_{i-1}^{k_{i-1}} p_{i+1}^{k_{i+1}} \cdots p_t^{k_t} y =$$

$$= p_1^{k_1} \cdots p_{i-1}^{k_{i-1}} p_{i+1}^{k_{i+1}} \cdots p_t^{k_t} (y_1 + \cdots + y_{i-1} + y_{i+1} + \cdots + y_t)$$

$$= p_1^{k_1} \cdots p_{i-1}^{k_{i-1}} p_{i+1}^{k_{i+1}} \cdots p_t^{k_t} y_1 + \cdots + p_1^{k_1} \cdots p_{i-1}^{k_{i-1}} p_{i+1}^{k_{i+1}} \cdots p_t^{k_t} y_{i-1}$$

$$+ p_1^{k_1} \cdots p_{i-1}^{k_{i-1}} p_{i+1}^{k_{i+1}} \cdots p_t^{k_t} y_{i+1} + \cdots + p_1^{k_1} \cdots p_{i-1}^{k_{i-1}} p_{i+1}^{k_{i+1}}$$

$$\cdots p_t^{k_t} y_t = 0.$$

故有

$$p_i^{k_i} \in ann y, \quad p_1^{k_1} \cdots p_{i-1}^{k_{i-1}} p_{i+1}^{k_{i+1}} \cdots p_t^{k_t} \in ann y$$

由于

$$(p_i^{k_i},\ p_1^{k_1} \cdots p_{i-1}^{k_{i-1}} p_{i+1}^{k_{i+1}} \cdots p_t^{k_t}) = 1,$$

从而必有

$$1 \in ann y \Longrightarrow 1 \cdot y = 0 \Longrightarrow y = 0.$$

即得 $M_{p_i} \cap M_{p_1} + \cdots + M_{p_{i-1}} + M_{p_{i+1}} + \cdots + M_{p_t} = \{0\}$。

亦即证明了

$$M_{p_1} + M_{p_2} + \cdots + M_{p_t} = M_{p_2} \oplus M_{p_2} \oplus \cdots \oplus M_{p_t}. \ ∎$$

定理 5 设

$$M = Rx_{11} \oplus Rx_{12} \oplus \cdots \oplus Rx_{1r_1} \oplus$$
$$\oplus Rx_{21} \oplus Rx_{22} \oplus \cdots \oplus Rx_{2r_2} \oplus$$
$$\oplus \cdots \oplus$$
$$\oplus Rx_{s1} \oplus Rx_{s2} \oplus \cdots \oplus Rx_{sr_s},$$

为M的任意一个以准素循环模为项的直和分解式。其中

$$annx_{11} = (p_1^{e_{11}}),\ annx_{12} = (p_1^{e_{12}}),\ \cdots, annx_{1r_1} = (p_1^{e_{1r_1}}),$$

$$annx_{21} = (p_2^{e_{21}}), annx_{22} = (p_2^{e_{22}}), \cdots, annx_{2r_2} = (p_2^{e_{2r_2}}),$$

$$\vdots$$

$$annx_{s1} = (p_s^{e_{s1}}),\ annx_{s2} = (p_s^{e_{s2}}), \cdots, annx_{sr_s} = (p_s^{e_{sr_s}}),$$

而 p_1，p_2，…，p_s 为不同的素元素。那么

（1）$M = M_{p_1} \oplus M_{p_2} \oplus \cdots \oplus M_{p_s}$，

（2）$M_{p_t} = Rx_{t1} \oplus Rx_{t2} \oplus \cdots \oplus Rx_{tr_t}$，　$t = 1, 2, \cdots, s$。

证　先证（1）成立。由于$Rx_{ti_t} \subseteq M_{p_t}$，从而有

$$Rx_{t1} + Rx_{t2} + \cdots + Rx_{tr_t} \subseteq M_{p_t},$$

$$\Longrightarrow M \subseteq M_{p_1} + M_{p_2} + \cdots + M_{p_s}.$$

但显然有 $M_{p_1} + M_{p_2} + \cdots + M_{p_s} \subseteq M$，故得

$$M = M_{p_1} + M_{p_2} + \cdots + M_{p_s}.$$

再由命题3之（2），即得

$$M = M_{p_1} \oplus M_{p_2} \oplus \cdots \oplus M_{p_S}.$$

再证（2）成立。按M_{p_t}的定义，显然有

$$Rx_{t1} \oplus Rx_{t2} \oplus \cdots \oplus Rx_{tr_t} \subseteq M_{p_t}.$$

于是由题设以及刚证明过的（1），自然可得

$$Rx_{t1} \oplus Rx_{t2} \oplus \cdots \oplus Rx_{tr_t} = M_{p_t}.$$

即（2）成立。∎

推论 在定理5的前提下，若p为异于$p_1, p_2, \cdots, p_s$的素元素，则有$M_p=\{0\}$。

事实上，当p为异于$p_1, p_2, \cdots, p_s$的素元时，则有

$$M_p+M_{p_1}+M_{p_2}+\cdots+M_{p_s}=M_p\oplus M_{p_1}\oplus M_{p_2}\oplus\cdots\oplus M_{p_s}.$$

从而 $M_p\cap M_{p_1}\oplus+M_{p_2}\oplus\cdots\oplus M_{p_s}=\{0\}$。这样，由定理5之（1），即有

$$M_p\cap M=\{0\}\Longrightarrow M_p=\{0\}.\ ∎$$

最后，我们来证明标准分解式的唯一性。

定理 6 设M为主理想环R上的有限生成模，它有如下的两个标准分解式：

$$\begin{aligned}M&=Rz_1\oplus Rz_2\oplus\cdots\oplus Rz_S\\&=Rw_1\oplus Rw_2\oplus\cdots\oplus Rw_t,\end{aligned}$$

其中

$$ann z_1\supseteq ann z_2\supseteq\cdots\supseteq ann z_s,$$

$$ann w_1\supseteq ann w_2\supseteq\cdots\supseteq ann w_t,$$

并且分解式中均没有等于零的项。那么 $s=t$，

并且

$$ann z_1=ann w_1,\quad ann z_2=ann w_2,\quad\cdots,\quad ann z_s=ann w_s.$$

证 （一）归结于扭模的情形。

设 $ann z_1\neq 0, \cdots, ann z_r\neq 0$,

$ann z_{r+1}=0, \cdots, ann z_s=0$;

$ann w_1\neq 0, \cdots, ann w_u\neq 0$,

$ann w_{u+1}=0\cdots, ann w_t=0$.

于是

$$\begin{aligned}torM&=Rz_1\oplus Rz_2\oplus\cdots\oplus Rz_r\\&=Rw_1\oplus Rw_2\oplus\cdots\oplus Rw_u.\end{aligned}$$

从而

$$M/torM \simeq Rz_{r+1} \oplus \cdots \oplus Rz_s$$
$$\simeq Rw_{u+1} \oplus \cdots \oplus Rw_t,$$

其中的两个直和分别是秩为 $s-r$ 与 $t-u$ 的自由模。由于同构的自由模必有相同的秩数，所以

$$s-r=t-u.$$

即阶理想 $annz_i$ 中等于零的个数与阶理想 $annw_j$ 中等于零的个数相等。从而，这就使得定理 6 的证明归结为$M=torM$的情形。

（二）归结于 p—分支的情形。

设M为扭模，即 $M=torM$。我们考虑M的两种分解形式，即M的标准分解式与M的以准素循环模为项的直和分解式。前面已经说明，M的这样两种分解式可以互相唯一确定。因此，如果我们能指出M的任意两个以准素循环子模为项的直和分解式有相同的阶理想集合，那么在这两个分解式里，对任意一个素元素的幂p^e，以 (p^e) 为阶理想的准素循环子模的直和项的个数相同。于是定理 6 对扭模就成立。而要做到这一点，我们来考虑固定一个素元素 p。在两个分解式里，把有阶理想 (p^e) （$e=1, 2, \cdots$）的准素循环子模的一切项组成和。于是得到两个和，据 M_p 的定义与定理 5 可知，这两个和都是直和且都等于 M_p。因此，若对每一个 M_p 能证明：任意两个以准素循环子模为项的直和分解式中，项数相同，阶理想集合也相同，那么定理就被证明了。因而这又把定理 6 的证明归结为$M=M_p$的情形。

（三）对$M=M_p$的情形证明定理 6 成立。

设 $M=M_p=Rz_1\oplus Rz_2\oplus\cdots\oplus Rz_s$
$=Rw_1\oplus Rw_2\oplus\cdots\oplus Rw_t$.

于是

$$annz_1=(p^{e_1}), annz_2=(p^{e_2}), \cdots, annz_s=(p^{e_s}),$$

$$annw_1=(p^{f_1}), annw_2=(p^{f_2}), \cdots, annw_t=(p^{f_t}).$$

由于阶理想是递降的，可知

$$e_1\leqslant e_2\leqslant\cdots\leqslant e_s,\ f_1\leqslant f_2\leqslant\cdots\leqslant f_t.$$

令

$$p^kM=\{p^kx|x\in M\},\ k=0,\ 1,\ 2,\ \cdots.$$

则得子模的递降序列：

$$M\supseteq pM\supseteq p^2M\supseteq\cdots.$$

考虑商模

$$M^{(k)}=p^kM\Big/p^{k+1}M=\{p^kx+p^{k+1}M\,|\,x\in M\}.$$

商模$M^{(k)}$的任意元素 $\overline{p^kx}=p^kx+p^{k+1}M$与 R 中的元素 p 相乘，则有

$$p\cdot\overline{p^kx}=p(p^kx+p^{k+1}M)=p^{k+1}M=\overline{0}.$$

这表明环 R 的理想（p）零化模 $M^{(k)}$. 于是，按自然的方式可以把$M^{(k)}$看做商环$R/(p)$上的模. 因为 p 是素元素，所以$R/(p)$是域. 这样，$M^{(k)}$就成了域上的线性空间. 从而有一个确定的维数. 下面我们来分析线性空间$M^{(k)}$的维数与序列

$$e_1\leqslant e_2\leqslant\cdots\leqslant e_s$$

的联系. 为此考虑这样的 k：

$$e_1\leqslant e_2\leqslant\cdots\leqslant e_i\leqslant k<e_{i+1}\leqslant\cdots\leqslant e_s.$$

这就是说，序列 $e_1\leqslant e_2\leqslant\cdots\leqslant e_s$中有 $s-i$ 个数是大于 k 的. 于是

$$\begin{aligned}p^kM&=p^k(Rz_1\oplus\cdots\oplus Rz_i\oplus Rz_{i+1}\oplus\cdots\oplus Rz_s)\\&=R(p^kz_{i+1})\ +\cdots+R(p^kz_s)\ .\end{aligned}$$

由此可以看出，$\overline{p^kz_{i+1}}$，…，$\overline{p^kz_s}$，这 $s-i$个元素是域$R/(p)$上的线性空间 $M^{(k)}$ 的一组生成元素. 进而还不难指出这组生成元素是 $M^{(k)}$ 的一个基底. 为此令

$$\overline{b_{i+1}}\ \overline{p^kz_{i+1}}+\cdots+\overline{b_s}\ \overline{p^kz_s}=\overline{0},$$

其中系数$\overline{b_{i+1}}$，…，$\overline{b_s}$均为域 $R/(p)$中的元素。我们需要的是它们都是 $R/(p)$中之零元素。为了达到这个目的，我们把上面那个线性组合的式子改写成另外的形式，即

$$b_{i+1}p^k z_{i+1}+\cdots+b_s p^k z_s \in p^{k+1}M.$$

从而又可写成如下的等式：

$$b_{i+1}p^k z_{i+1}+\cdots+b_s p^k z_s = c_{i+1}p^{k+1}z_{i+1}+\cdots+c_s p^{k+1}z_s,$$

$$\Longrightarrow (b_{i+1}-c_{i+1}p)p^k z_{i+1}+\cdots+(b_s-c_s p)p^k z_s=0.$$

于是由定理1的证明过程，可知

$$(b_h-c_h p)p^k z_h=0,\ h=i+1,\ \cdots,\ s.$$

由此可得

$$p^{e_{i+1}}\diagdown(b_{i+1}-c_{i+1}p)p^k,\ \cdots,\ p^{e_s}\diagdown(b_s-c_s p)p^k.$$

因为$k<e_{i+1}\leqslant\cdots\leqslant e_s$，则有

$$p\diagdown(b_{i+1}-c_{i+1}p),\ \cdots,\ p\diagdown(b_s-c_s p)$$

$$\Longrightarrow p\diagdown b_{i+1},\ \cdots,\ p\diagdown b_s,$$

$$\Longrightarrow \overline{b_{i+1}}=\overline{0},\ \cdots,\ \overline{b_s}=\overline{0}$$

此处$\overline{0}$是域$R/(p)$的零元素。

这就说明$\overline{p^k z_{i+1}}$，…，$\overline{p^k z_s}$在 $R/(p)$ 上是线性无关的，即$\overline{p^k z_{i+1}}$，…，$\overline{p^k z_s}$是线性空间$M^{(k)}$的一个基底。故而$M^{(k)}$的维数等于 $s-i$。

总括起来说，即有

对任意一个非负整数 k，数列 e_1，e_2，…，e_s中大于k的数的个数恰好等于$M^{(k)}$的维数。

当然，完全同样的，也有

对任意一个非负整数 k，数列f_1，f_2，…，f_t中大于k的数的个数恰好等于$M^{(k)}$的维数。

由此必有

$s=t$，并且 $e_1=f_1$，$e_2=f_2$，…，$e_s=f_s$。

这就完全证明了定理 6。▌

我们把刚才证明是唯一的阶理想递降序列

$$\mathrm{ann}z_1, \ \mathrm{ann}z_2, \ \cdots, \ \mathrm{ann}z_s$$

叫做模M的**不变因子理想**。

在M的以准素循环模为项的直和分解式中，各个准素循环子模的阶理想叫做M的**初等因子理想**。使用这样两个术语，便有

定理 7 主理想环 R上两个有限生成模是同构的$\Longleftrightarrow$它们有相同的不变因子理想。▌

定理 8 主理想环 R上的两个有限生成的扭模是同构的$\Longleftrightarrow$它们有相同的初等因子理想。▌

在 $R=Z$ 时，每个理想有唯一的非负生成元素；在 $R=F[\lambda]$（F 为域）时，每个理想也是或者由零元生成，或者由唯一的一个首系数等于 1 的多项式生成。在 R是这两种特殊的环的情形，自然的把不变因子理想的唯一确定的生成元素叫做模的**不变因子**；而把初等因子理想组中各个理想的唯一确定的生成元素叫做模的**初等因子**。

习　题

1. 试决定$Z^{(3)}/K$的结构，其中K是由

$$f_1=(2, 1, -3),$$
$$f_2=(1, -1, 2),$$

生成的子模。

2. 设 D是高斯整数环$Z[i]$。试决定 $D^{(3)}/K$的结构，其中

$f_1=(1, 3, 6)$,

$f_2=(2+3i, -3i, 12-18i)$,

$f_3=(2-3i,\ 6+9i,\ -18i)$

为子模K的一组生成元。

3．如果M是由 2 与 x 生成的$Z[x]$的理想子环，试证M不能表成循环 $Z[x]$——模的直和。

4．设 D为实数域R上的多项式环$R[\lambda]$，M是 D——模，表成循环模的直和：

$$M=Dy_1\oplus Dy_2\oplus Dy_3\oplus Dy_4,$$

其中

$$y_1=(\lambda-1)^3, \qquad y_2=(\lambda^2+1)^2,$$

$$y_3=(\lambda-1)(\lambda^2+1)^4, \qquad y_4=(\lambda+2)(\lambda^2+1)^2.$$

试决定M的初等因子和不变因子。

5．试证主理想环 D 上的扭模 M 是不可约的当且仅当 $M=Dz$，$annz=(p)$，其中p为D中的素元。

6．设M是主理想环D上的有限生成模。试证：M 是不可分解的当且仅当$M=Dz$，$annz=(p^e)$，其中 p 是 D 中之素元。

7．我们把主理想环 D上的有限生成模M的秩定义为自由模$M/torM$的秩。试证：

如果$M\simeq D^{(n)}/K$，那么$rankM=n-rankK$。

并且

如果N是M的一个子模，那么N与M/N都是有限生成的，而且有

$$rankM=rankN+rankM/N.$$

8．设M是主理想环D上的扭模，不变因子理想序列为

$$(d_1)\supseteq(d_2)\supseteq\cdots\supseteq(d_s)$$

证明：M的任意一个同态象$\overline{M}$也是扭模，并且$\overline{M}$有不变因子理想序列为

$$(\overline{d_1})\supseteq(\overline{d_2})\supseteq\cdots\supseteq(\overline{d_t}),$$

使得 $t\leqslant s$，以及$\overline{d_t}\diagdown d_s$，$\overline{d_{t-1}}\diagdown d_{s-1}$，…，$\overline{d_1}\diagdown d_{s-t+1}$。

9．设M是主理想环 D上的模，N 是M的一个子模，如果对

于任意的 $a\in D$，$y\in N$，使得

$$ax=y\text{在}M\text{中可解}\Longleftrightarrow ax=y\text{在}N\text{中可解},$$

则称 N是M的纯子模。试证：

1）如果子模N是M的直和项，那么N是M的纯子模。

2）如果N是M的一个纯子模，以及

$$ann(x+N)=(d),$$

那么陪集$x+N$中存在元素x，使$annx=(d)$。

10. 证明：如果N是主理想环 D上有限生成的扭模M的一个纯子模，那么N是M的直和项。

11. 设M是主理想环 D上的有限生成的扭模。证明：对每一个$x\in M$，任意一个使

$$annz\subseteq annx$$

的循环子模Dz是M的一个纯子模，从而Dz是M的一个直和项。

§5 在交换群和线性变换上的应用

本节把主理想环 R上有限生成模的结构理论应用于两个特殊的情形，即$R=Z$与$R=F$的情形，此处F是域。

首先考察$R=Z$的情形。

这时模M就是通常的有有限生成组的交换群。于是，基本结构定理（§ 4 定理 1）表明：

有限生成的交换群M是循环群的直和：

$$M=[z_1]\oplus[z_2]\oplus\cdots\oplus[z_s],$$

其中$\mathrm{ann}z_1=(d_1)$，$\mathrm{ann}z_2=(d_2)$，…，$\mathrm{ann}z_s=(d_s)$，且使

$$d_1\diagdown d_2\diagdown\cdots\diagdown d_s.$$

如果令 $d_i\geqslant 0$ $(i=1,2,\cdots,s)$，那么d_i就正是z_i的阶（周期）。假设

$$d_1\neq 0,\ d_2\neq 0,\ \cdots,\ d_r\neq 0,\ d_{r+1}=0,\ \cdots,\ d_s=0,$$

于是群M的扭子群就是 M中一切有限阶元素组成的子群，而且有

$$torM=[z_1]\oplus[z_2]\oplus\cdots\oplus[z_r].$$

显然，$torM$中恰好含有$d_1d_2\cdots d_r$个元素，即

$$|torM|=d_1d_2\cdots d_r.$$

这说明任意有限生成的交换群M的“扭”$torM$ 只含有限个元素。并且使

$$M=torM\oplus M_0,$$

其中 M_0 是一个自由群。一般来说，这个“自由成份”不是唯一确定的。但是它的秩数是唯一的。显然，M_0是个无限群，其中没有阶为有限的元素了。

关于扭模分解成准素循环模的直和的一般结果（§ 4定理4），在此特殊化为：

任意有限交换群M是阶为素数幂的循环群的直和。并且，做

为这个分解式中各项的阶的各素数幂及每一个幂p^e的个数都是唯一确定的，称这样确定的素数幂为群M的不变量。于是有

两个有限交换群是同构的$\Longleftrightarrow$它们有相同的不变量。

例如，据此结果容易断言：6阶交换群只有1个。这是因为$6=2\times3$，所以6的素数幂因子只有一种分配方式，即

$$2,\ 3.$$

因此，6阶交换群就是

$$M=Z_2\oplus Z_3,$$

其中 $Z_2=\{\overline{0},\ \overline{1}\}$，$Z_3=\{\overline{0},\ \overline{1},\ \overline{2}\}$。当然

$$Z_2\oplus Z_3\simeq Z_6=\{\overline{0},\ \overline{1},\ \overline{2},\ \overline{3},\ \overline{4},\ \overline{5}\}.$$

同样可以断言：4阶交换群只有两个。这是因为$4=2^2$，所以4的不同的素数幂因子有两种分配方式：

（1）2，2；

（2）2^2。

因此，4阶交换群有如下两个：

$$M_1=Z_2\oplus Z_2;\quad M_2=Z_4.$$

其中M_1就是 *klein* 四元群。

其次研究$R=F$是域的情形。

这时域F上的有限生成模就是F上的有限维线性空间。由此我们可以得到有限维线性空间上一个线性变换σ的标准形理论。

设V是域F上的n维空间，σ是V上的任意一个取定的线性变换。任意取定V的一个基底u_1，u_2，…，u_n。即有

$$V=[u_1,\ u_2,\ \cdots,\ u_n].$$

令线性变换σ在基底u_1，u_2，…，u_n上的系数阵为$A=(a_{ij})$。则有

$$\sigma\begin{pmatrix}u_1\\u_2\\\vdots\\u_n\end{pmatrix}=\begin{pmatrix}\sigma u_1\\\sigma u_2\\\vdots\\\sigma u_n\end{pmatrix}=A\begin{pmatrix}u_1\\u_2\\\vdots\\u_n\end{pmatrix},$$

这时 σu_i 用基底 $u_1, u_2, \cdots, u_n$ 线性表出的系数恰好是矩阵 $A=(a_{ij})$ 的第 i 行元素。

众所周知，如果以可逆矩阵P为过渡阵把基底 $u_1, u_2, \cdots, u_n$换成新的基底$v_1, v_2, \cdots, v_n$，即有

$$\begin{pmatrix} v_1 \\ v_2 \\ \vdots \\ v_n \end{pmatrix} = P \begin{pmatrix} u_1 \\ u_2 \\ \vdots \\ u_n \end{pmatrix}.$$

于是，线性变换 σ 关于这个新基底的系数矩阵就是

$$B = PAP^{-1}.$$

即线性变换 σ 关于两个基底的系数矩阵是相似的，具体联系如上式。

一个线性变换 σ 在两个基底上的系数矩阵之间的这种联系提示了一种可能性，即如果可逆矩阵 P选取得适当，可以使 B具有相当简单的形式。这就是有名的相似标准形问题。

为了解决上述的标准形问题，我们回忆起以下的情况：用给定的线性变换 σ 可以把原本是域 F 上的 n 维线性空间V定义成多项式环$F[\lambda]$上的有限生成模。这里的关键是弄清楚作为环$F[\lambda]$上的模 V，倍数乘法是怎样施行的。

对于$F[\lambda]$中的任意一个元素：

$$g(\lambda) = b_0 + b_1\lambda + \cdots + b_m\lambda^m,$$

和V中的任意一个元素x，用$g(\lambda)$去乘 x 的乘法，规定为

$$g(\lambda)x = b_0x + b_1(\sigma x) + \cdots + b_m(\sigma^m x),$$

即

$$g(\lambda)x = g(\sigma)x.$$

显然，$F[\lambda]$ 与 V 之间的倍数乘法是 F与V 之间的倍数乘法的扩充，且使 $\lambda x = \sigma x$。

以下我们用上一节的结构理论来具体分析 $F[\lambda]$—模 V 的结构。

首先，由$V=[u_1, u_2, \cdots, u_n]$，可知做为$F[\lambda]$上的模来看$V$是有限生成的，$u_1, u_2, \cdots, u_n$就是$V$在$F[\lambda]$上的一组生成元素。即有

$$V=F[\lambda]u_1+F[\lambda]u_2+\cdots+F[\lambda]u_n.$$

其次 $torV=V$，即V是$F[\lambda]$上的扭模。换句话说，V中任一元素x在$F[\lambda]$里的零化子均不等于$\{0\}$，即$annx\neq 0$。

事实上，若$x\in V$，那么由于V是F上的n维空间，于是对序列，

$$x, \lambda x, \lambda^2 x, \cdots$$

来说，一定有正整数 $m\leqslant n$，使$\lambda^m x$是

$$x, \lambda x, \cdots, \lambda^{m-1}x$$

的线性组合。即有

$$\lambda^m x=b_0x+b_1\lambda x+\cdots+b_{m-1}\lambda^{m-1}x,\quad b_i\in F.$$

于是，有非零多项式

$$g(\lambda)=\lambda^m-b_{m-1}\lambda^{m-1}-\cdots-b_1\lambda-b_0,$$

使

$$g(\lambda)x=0.$$

从而 $g(\lambda)\in annx$，因此$annx\neq 0$。

对于这个有限生成的扭模V，自然有$F[\lambda]$上的自由模

$$F[\lambda]^{(n)}=[e_1, e_2, \cdots, e_n],$$

使得

$$F[\lambda]^{(n)}\overset{\eta}{\sim}V,$$

其中

$$\eta: e_i\longmapsto u_i,\quad i=1, 2, \cdots, n.$$

从而

$$F[\lambda]^{(n)}/K\simeq V,\quad K=ker\eta.$$

为了用$F[\lambda]^{(n)}/K$的结构来决定V的结构，我们需要取K的一个生成组。对此我们可以证明如下的

命题 元素

$$f_i = \lambda e_i - \sum_{j=1}^{n} a_{ij} e_j,\quad 1 \leqslant i \leqslant n,$$

是 K的一个基底。

证 首先指出f_i都是K中的元素。这只须说明f_i在η之下的象都是V中的零元。

事实上

$$\begin{aligned}\eta(f_i) &= \eta(\lambda e_i - \sum_{j=1}^{n} a_{ij} e_j) \\ &= \lambda\eta(e_i) - \sum_{j=1}^{n} a_{ij}\eta(e_j) \\ &= \lambda u_i - \sum_{j=1}^{n} a_{ij} u_j \\ &= \lambda u_i - \sigma u_i \\ &= \sigma u_i - \sigma u_i \\ &= 0.\end{aligned}$$

其次指出 $f_1, f_2, \cdots, f_n$是K的一组生成元。

因为$F[\lambda]^{(n)}$中之任意一个元素y都可以表成基底 $e_1, e_2,$ e_n的线性组合：

$$y = g_1(\lambda)e_1 + g_2(\lambda)e_2 + \cdots + g_n(\lambda)e_n.$$

而由 $f_i = \lambda e_i - \sum_{j=1}^{n} a_{ij} e_j$，即有

$$\lambda e_i = f_i + \sum_{j=1}^{n} a_{ij} e_j$$

可使 y 表成以下的形式：

$$y = \sum h_i(\lambda) f_i + \sum b_i e_i.$$

于是

$$y\in K\Longleftrightarrow\sum b_ie_i\in K\Longleftrightarrow\sum b_iu_i=0\Longleftrightarrow b_i=0.$$

这样，$y\in \bar{K}\Longleftrightarrow y=\sum h_i(\lambda)f_i$。即$f_1$，$f_2$，…，$f_n$是$K$的一组生成元素。

最后再指出f_1，f_2，…，f_n在$F[\lambda]$上是线性无关的，对此，如果

$$\sum_{i=1}^{n}h_i(\lambda)f_i=0,$$

用$f_i=\lambda e_i-\sum_{j=1}^{n}a_{ij}e_j$代入上式，则有

$$\sum_{i=1}^{n}h_i(\lambda)\lambda e_i=\sum_{i,j=1}^{n}h_i(\lambda)a_{ij}e_j$$

由此可得

$$h_i(\lambda)\lambda=h_1(\lambda)a_{1i}+h_2(\lambda)a_{2i}+\cdots+h_n(\lambda)a_{ni}.$$

其中$i=1,2,\cdots,n$。

上式只有当每一$h_i(\lambda)$均等于零时才能成立。否则不妨认为$h_1(\lambda)$是次数最大的一个。这时，我们看：

$$h_1(\lambda)\lambda=h_1(\lambda)a_{11}+h_2(\lambda)a_{21}+\cdots+h_n(\lambda)a_{n1}$$

从而可见，左端的次数为$\deg h_1(\lambda)+1$，而右端的次$\leqslant\deg h_1(\lambda)$。这是个矛盾，它表明必须一切$h_i(\lambda)$均等于零。这就证明了$f_1$，$f_2$，…，$f_n$是子模$K$的一个基底。█

这样，我们容易知道，子模K的这个基底$f_1,f_2,\cdots,f_n$用模$F[\lambda]^{(n)}$的基底e_1，e_2，…，e_n线性表出时恰好有以下的形式：

$$\begin{pmatrix}f_1\\f_2\\\vdots\\f_n\end{pmatrix}=\begin{pmatrix}\lambda-a_{11}&-a_{12}&\cdots&-a_{1n}\\-a_{21}&\lambda-a_{22}&\cdots&-a_{2n}\\\cdot&\cdot&\cdots&\cdot\\-a_{n1}&-a_{n2}&\cdots&\lambda-a_{nn}\end{pmatrix}\begin{pmatrix}e_1\\e_2\\\vdots\\e_n\end{pmatrix}$$

其中系数矩阵为

$$\lambda I - A = \begin{pmatrix} \lambda - a_{11} & -a_{12} & \cdots & -a_{1n} \\ -a_{21} & \lambda - a_{22} & \cdots & -a_{2n} \\ \cdot & \cdot & \cdots & \cdot \\ -a_{n1} & -a_{n2} & \cdots & \lambda - a_{nn} \end{pmatrix}.$$

它正好如通常所说的是线性变换 σ 的系数矩阵A的特征矩阵。同时称行列式

$$|\lambda I - A| = f(\lambda) = \lambda^n - a_1\lambda^{n-1} + \cdots + (-1)^n a_n$$

为矩阵 A的**特征多项式。**

于是，由 § 4 定理 1 的证明过程可知，特征矩阵$\lambda I - A$的不变因子恰好就是 $F[\lambda]$—模 V 的不变因子，并且所有不变因子的积等于特征多项式 $f(\lambda)$ 。

由于V是 $F[\lambda]$ 上的扭模，所以 $\lambda I - A$ 的标准形必有以下形式：

$$\begin{pmatrix} 1 & & & & & & \\ & \ddots & & & & & \\ & & 1 & & & & \\ & & & d_1(\lambda) & & & \\ & & & & d_2(\lambda) & & \\ & & & & & \ddots & \\ & & & & & & d_s(\lambda) \end{pmatrix}$$

其中 $d_1(\lambda)$, $d_2(\lambda)$, $\cdots$, $d_S(\lambda)$ 都是首系数等于 1 的多项式，并且依次能整除，即有

$$d_1(\lambda) \diagdown d_2(\lambda) \diagdown \cdots \diagdown d_S(\lambda).$$

于是，存在可逆矩阵 P, Q, 使

$$Q(\lambda I - A)P = \begin{pmatrix} 1 & & & & & & \\ & \ddots & & & & & \\ & & 1 & & & & \\ & & & d_1(\lambda) & & & \\ & & & & d_2(\lambda) & & \\ & & & & & \ddots & \\ & & & & & & d_s(\lambda) \end{pmatrix}.$$

这样令

$$\begin{pmatrix} v_1 \\ v_2 \\ \vdots \\ v_n \end{pmatrix} = P^{-1} \begin{pmatrix} u_1 \\ u_2 \\ \vdots \\ u_n \end{pmatrix},$$

并取

$$z_1 = v_{n-s+1}\ ,\ z_2 = v_{n-s+2}\ ,\ \cdots,\quad z_{s-1} = v_{n-1},\ z_s = v_n.$$

便得$F[\lambda]$—模V的标准分解式：

$$V = F[\lambda]z_1 \oplus F[\lambda]z_2 \oplus \cdots \oplus F[\lambda]z_s,$$

其中

$$annz_1 = (d_1(\lambda)),\ annz_2 = (d_2(\lambda))\ ,\ \cdots, annz_s = (d_s(\lambda))\ .$$

以下我们通过$F[\lambda]$—模 V 的这个标准分解式找出线性变换σ的表示矩阵 A的相似标准形。

首先，当$s=1$时，$V = F[\lambda]z_1$是循环模．于是

$$annz_1 = (d_1(\lambda))\ =\ (f(\lambda))\ ,$$

此处$f(\lambda)$ 是A的特征多项式，由于$f(\lambda)$ 是零化z_1的次数最低的非零多项式。从而可以断定

$$z_1,\ \lambda z_1,\ \cdots,\ \lambda^{n-2}z_1,\ \lambda^{n-1}z_1$$

这 n 个元素必为F—空间V中 n 个线性无关的向量。而V在 F上的维数等于n，因此 z_1，λz_1，…，$\lambda^{n-2}z_1$，$\lambda^{n-1}z_1$ 是 V 的一个基底。

我们来求出线性变换 σ 在 V 的这个基底上的系数矩阵。我们有

$$\sigma z_1 = \lambda z_1,$$
$$\sigma(\lambda z_1) = \lambda(\sigma z_1) = \lambda^2 z_1,$$
$$\vdots$$
$$\sigma(\lambda^{n-2}z_1) = \lambda^{n-2}(\sigma z_1) = \lambda^{n-1}z_1,$$
$$\sigma(\lambda^{n-1}z_1) = \lambda^{n-1}(\sigma z_1) = \lambda^n z_1$$
$$= a_1\lambda^{n-1}z_1 - a_2\lambda^{n-2}z_1 + \cdots + (-1)^{n-1}a_n z_1$$

由此可得σ在z_1，λz_1，…，$\lambda^{n-2}z_1$，$\lambda^{n-1}z_1$上的系数矩阵为

$$\begin{pmatrix} 0 & 1 & 0 & \cdots & 0 & 0 \\ 0 & 0 & 1 & \cdots & 0 & 0 \\ \cdot & \cdot & \cdot & \cdots & \cdot & \cdot \\ 0 & 0 & 0 & \cdots & 0 & 1 \\ (-1)^{n-1}a_n & \cdot & \cdot & \cdots & -a_2 & a_1 \end{pmatrix}$$

这个矩阵的最后一行恰好是 $d_1(\lambda)(=(f(\lambda))$ 的除去首系数之外的系数反号之后，按升幂的顺序排列而成。

一般地，对任意一个首项系数等于1的多项式：

$$d(\lambda)=\lambda^m-b_{m-1}\lambda^{m-1}-\cdots-b_1\lambda-b_0,$$

都唯一的确定一个形如

$$\begin{pmatrix} 0 & 1 & 0 & \cdots & 0 & 0 \\ 0 & 0 & 1 & \cdots & 0 & 0 \\ \cdot & \cdot & \cdot & \cdots & \cdot & \cdot \\ 0 & 0 & 0 & \cdots & 0 & 1 \\ b_0 & b_1 & b_2 & \cdots & b_{m-2} & b_{m-1} \end{pmatrix}$$

的矩阵，称其为多项式$d(\lambda)$ 的**伴随矩阵**。用这样的术语便有：上述线性变换 σ 关于基底，

$$z_1,\ \lambda z_1,\ \cdots,\ \lambda^{n-2}z_1,\ \lambda^{n-1}z_1$$

的系数矩阵正是特征多项式$f(\lambda)$ 的伴随矩阵。

现在考虑一般情形。

这时我们对 V的标准分解式

$$V=F[\lambda]z_1\oplus F[\lambda]z_2\oplus\cdots\oplus F[\lambda]z_s$$

中的每一个循环子模$F[\lambda]z_i$，求出它在F上的基底。把这些子模的基底依次按段连在一起就正好是V在F上的一个基底。

设 $d_i(\lambda)$ 的次数为n_i，则

$$z_i,\ \lambda z_i,\ \cdots,\ \lambda^{n_i-1}z_i$$

就是子模 $F[\lambda]z_i$ 在 F 上的一个基底。令

$$d_i(\lambda)=\lambda^{n_i}-b_{i\,n_i-1}\lambda^{n_i-1}-\cdots-b_{i1}\lambda-b_{i0},$$

则有

$$\sigma z_i = \lambda z_i,$$
$$\sigma(\lambda z_i) = \lambda^2 z_i,$$
$$\vdots$$
$$\sigma(\lambda^{n_i-2} z_i) = \lambda^{n_i-1} z_i,$$
$$\sigma(\lambda^{n_i-1} z_i) = \lambda^{n_i} z_i = b_{i0} z_i + b_{i1}(\lambda z_i) + \cdots + b_{i n_i-1}(\lambda^{n_i-1} z_i).$$

因此，σ在子模 $F[\lambda]z_i$ 上看时，关于基底 z_i，$\lambda z_i,\cdots,\lambda^{n_i-1}z_i$ 的系数矩阵为

$$B_i = \begin{pmatrix} 0 & 1 & 0 & \cdots & 0 & 0 \\ 0 & 0 & 1 & \cdots & 0 & 0 \\ \cdot & \cdot & \cdot & \cdots & \cdot & \cdot \\ 0 & 0 & 0 & \cdots & 0 & 1 \\ b_{i0} & b_{i1} & b_{i2} & \cdots & b_{in_i-2} & b_{in_i-1} \end{pmatrix}$$

于是 σ 关于V的基底

z_1，λz_1，$\cdots$，$\lambda^{n_1-1}z_1$，z_2，λz_2，$\cdots$，$\lambda^{n_2-1}z_2$，$\cdots$，z_s，λz_s，$\cdots$，$\lambda^{n_s-1}z_s$ 的系数矩阵为

$$B = \begin{pmatrix} B_1 & & & \\ & B_2 & & \\ & & \ddots & \\ & & & B_s \end{pmatrix},$$

其中B_i是$d_i(\lambda)$ 的伴随矩阵。把这样的矩阵B叫做线性变换 σ的**有理标准形**。

总结以上讨论，对于域F上 n 维线性空间V的线性变换σ，为了求出 σ 的有理标准形矩阵，具体步骤如下：

1）任意给出σ在V的某一基底u_1，u_2，$\cdots$，u_n 上的系数矩阵，设为 A。

2）用初等变换求特征矩阵 $\lambda I-A$的标准形如下：

$$B(\lambda)=\begin{pmatrix}1 & & & & & \\ & \ddots & & & & \\ & & 1 & & & \\ & & & d_1(\lambda) & & \\ & & & & d_1(\lambda) & \\ & & & & & \ddots \\ & & & & & & d_s(\lambda)\end{pmatrix},$$

从而得到A的非常数的不变因子$d_1(\lambda)$，$d_2(\lambda)$，…，$d_s(\lambda)$。

3）写出 $d_i(\lambda)$ 的伴随矩阵 B_i，$i=1, 2, \cdots, s$。那么对角形分块矩阵

$$B=\begin{pmatrix}B_1 & & & \\ & B_2 & & \\ & & \ddots & \\ & & & B_s\end{pmatrix}$$

就是 A 的有理标准形，亦即线性变换 σ 的有理标准形矩阵。

如果希望指出线性变换 σ 的这个有理标准形矩阵所依赖的基底，可以按如下的步骤进行：

1）把化特征矩阵 $\lambda I-A$ 为标准形的各个初等变换积累起来，表现为

$$Q(\lambda I-A)P=B(\lambda)=\begin{pmatrix}1 & & & & & \\ & \ddots & & & & \\ & & 1 & & & \\ & & & d_1(\lambda) & & \\ & & & & d_2(\lambda) & \\ & & & & & \ddots \\ & & & & & & d_s(\lambda)\end{pmatrix}$$

其中Q，P为 $F[\lambda]$上的可逆矩阵（实际上等于一些初等矩阵的乘积）

2）以P^{-1}为过渡矩阵，得出V在 $F[\lambda]$上的生成组

$$\begin{pmatrix}v_1\\ v_2\\ \vdots\\ v_n\end{pmatrix}=P^{-1}\begin{pmatrix}u_1\\ u_2\\ \vdots\\ u_n\end{pmatrix}$$

写出

$$z_1=v_{n-s+1}\ ,\ z_2=v_{n-s+2}\ ,\ \cdots,\ z_{s-1}=v_{n-1},\ z_s=v_n.$$

3）对于每一个 z_i（$i=1, 2, \cdots, s$）求出

$$z_i,\ \sigma z_i,\ \cdots,\ \sigma^{n_i-1}z_i.$$

其中 n_i是不变因子 $d_i(\lambda)$ 的次数。把这样得出的s组元素按段连接起来：

$z_1,\ \sigma z_1,\ \cdots,\ \sigma^{n_1-1}z_1,\ z_2,\ \sigma z_2,\ \cdots,\ \sigma^{n_2-1}z_2,\ \cdots,$ $z_s,\ \sigma z_s,\ \cdots,\ \sigma^{n_s-1}z_s$，这就是$V$在$F$上的一个基底。在这个基底上$\sigma$的系数矩阵就是有理标准形的。

例 设 $V=Q^{(3)}$是有理数域Q上的三数组空间，令u_1，u_2，u_3 是 V 的任一基底：$V=[u_1, u_2, u_3]$。

取V上的线性变换σ为

$$\sigma u_1=-u_1-2u_2+6u_3,$$
$$\sigma u_2=-u_1\qquad+3u_3,$$
$$\sigma u_3=-u_1-u_2+4u_3.$$

即σ 在基底u_1，u_2，u_3 上的系数矩阵为

$$A=\begin{pmatrix}-1 & -2 & 6\\ -1 & 0 & 3\\ -1 & -1 & 4\end{pmatrix}$$

试求A的有理标准形。或者说，求出线性变换σ的有理标准形矩阵。

解 按以上所说步骤去做。

1）题中已经给出σ在基底u_1，u_2，u_3 上的系数矩阵 A。

2）用初等变换求特征矩阵

$$\lambda I-A=\begin{pmatrix}\lambda+1 & 2 & -6\\ 1 & \lambda & -3\\ 1 & 1 & \lambda-4\end{pmatrix}$$

的标准形。具体过程我们略去不写，其结果是

$$Q(\lambda I-A)P=\begin{pmatrix}1 & & \\ & \lambda-1 & \\ & & (\lambda-1)^2\end{pmatrix}$$

其中

$$Q=\begin{pmatrix}0 & 1 & 0\\ 0 & -1 & 1\\ 1 & 2-\lambda & -3\end{pmatrix},\quad P=\begin{pmatrix}1 & 3 & \lambda-3\\ 0 & 0 & -1\\ 0 & 1 & -1\end{pmatrix}$$

是分别集中体现了上述化简过程中所用的行、列的初等变换。

这里有两个非常数的不变因子：

$$d_1(\lambda)=\lambda-1,\ d_2(\lambda)=\lambda^2-2\lambda+1.$$

3）写出 $d_1(\lambda)$ 与$d_2(\lambda)$ 的伴随矩阵：

$$B_1=(1),\quad B_2=\begin{pmatrix}0 & 1\\ -1 & 2\end{pmatrix},$$

从而 A 的有理标准形为

$$B=\begin{pmatrix}B_1 & \\ & B_2\end{pmatrix}=\begin{pmatrix}1 & 0 & 0\\ 0 & 0 & 1\\ 0 & -1 & 2\end{pmatrix}$$

如果希望指出线性空间$Q^{(3)}$的使线性变换σ的系数矩阵为上述的有理标准形的基底，可按前面指明的步骤去做。即

1）在前面化简过程中已经得出可逆矩阵

$$P=\begin{pmatrix}1 & 3 & \lambda-3\\ 0 & 0 & -1\\ 0 & 1 & -1\end{pmatrix}$$

2) 求出

$$P^{-1}=\begin{pmatrix}1 & \lambda & -3\\ 0 & -1 & 1\\ 0 & -1 & 0\end{pmatrix}$$

以 P^{-1}为过渡阵，写出

$$v_1=u_1+\lambda u_2-3u_3,$$
$$v_2=-u_2+u_3,$$
$$v_3=-u_2.$$

因为A的非常数的不变因子有两个，所以应有

$$z_1=v_2,\ z_2=v_3.$$

3）对 z_1，z_2 逐次求出“部分基底”：

$$z_1,\ z_2,\ \sigma z_2.$$

这样，z_1，z_2，σz_2 就是所求的基底。为了看得明白，把这个基底用V的原来的基底 u_1，u_2，u_3 表达出来如下：

$$z_1=v_2=-u_2+u_3,$$
$$z_2=v_3=-u_2,$$
$$\sigma z_2=\lambda z_2=\lambda v_3=-\lambda u_2=u_1-3u_3.$$

即有

$$\begin{cases} z_1= & -u_2+u_3,\\ z_2= & -u_2\qquad ,\\ \sigma z_2=u_1 & \qquad -3u_3. \end{cases}$$

于是，新、旧两个基底之间的过渡矩阵为

$$C=\begin{pmatrix}0 & -1 & 1\\ 0 & -1 & 0\\ 1 & 0 & -3\end{pmatrix}.$$

最后，利用这个过渡矩阵C也可得出线性变换σ的有理标准

形矩阵为

$$CAC^{-1}=\begin{pmatrix}0&-1&1\\0&-1&0\\1&0&-3\end{pmatrix}\begin{pmatrix}-1&-2&6\\-1&0&3\\-1&-1&4\end{pmatrix}\begin{pmatrix}3&-3&1\\0&-1&0\\1&-1&0\end{pmatrix}$$

$$=\begin{pmatrix}1&0&0\\0&0&1\\0&-1&2\end{pmatrix}$$

线性变换 σ 还可能存在另外一种标准形矩阵，即所谓的 *Jordan* 标准形。这需要每一个非常数的不变因子都能分解成 $F[\lambda]$ 中一次因式的乘积。如果 F 是复数域时，就能办到这一点。

现在假设 $F[\lambda]$ 中的非常数多项式都能分解成一次因式的乘积。这样，关于 $F[\lambda]$—模 V 的初等因子都有以下形式：

$$(\lambda-r)^e,\ r\in F.$$

对应每一个初等因子 $(\lambda-r)^e$，有一个准素的直和项：

$$F[\lambda]w,\ annw=((\lambda-r)^e)$$

因为 $(\lambda-r)^e$ 是 w 的化零多项式当中次数最低的，所以 $F[\lambda]$—模 $F[\lambda]w$ 做为 F 上的线性空间有基底为

$$w,\ (\lambda-r)w,\ (\lambda-r)^2w,\ \cdots,\ (\lambda-r)^{e-1}w.$$

并且有

$$\sigma w=\lambda w=rw+(\lambda-r)w,$$

$$\sigma(\lambda-r)w=\lambda(\lambda-r)w=r(\lambda-r)w+(\lambda-r)^2w.$$

$$\vdots$$

$$\sigma(\lambda-r)^{e-2}w=\lambda(\lambda-r)^{e-2}w=r(\lambda-r)^{e-2}w+(\lambda-r)^{e-1}w,$$

$$\begin{aligned}\sigma(\lambda-r)^{e-1}w&=\lambda(\lambda-r)^{e-1}w\\&=r(\lambda-r)^{e-1}w+(\lambda-r)^ew\\&=r(\lambda-r)^{e-1}w\end{aligned}$$

因此，把 σ 限制在 $F[\lambda]w$ 上来看时，σ 关于基底

$$w,\ (\lambda-r)w,\ \cdots,\ (\lambda-r)^{e-1}w$$

的系数矩阵是

$$\begin{pmatrix} r & 1 & 0 & \cdots & 0 & 0 \\ 0 & r & 1 & \cdots & 0 & 0 \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & 0 & \cdots & r & 1 \\ 0 & 0 & 0 & \cdots & 0 & r \end{pmatrix}$$

这样，当把V表成以准素循环模为项的直和为

$$V=F[\lambda]w_1\oplus F[\lambda]w_2\oplus\cdots\oplus F[\lambda]w_t$$

时，其中

$$\operatorname{ann} w_i=((\lambda-r_i)^{e_i}),\quad i=1,\ 2,\ \cdots,\ t.$$

那么对每一个准素的直和项 $F[\lambda]w_i$，做为F上的线性空间求出它的基底：

$$w_i,\ (\lambda-r_i)w_i,\ \cdots,\ (\lambda-r_i)^{e_i-1}w_i,\quad i=1,\ 2,\cdots,\ t.$$

把这t组“部分基”连在一起就得到线性空间V关于F的一个基底：

$$\begin{aligned} &w_1,\ (\lambda-r_1)w_1,\ \cdots,\ (\lambda-r_1)^{e_1-1}w_1, \\ &w_2,\ (\lambda-r_2)w_2,\ \cdots,\ (\lambda-r_2)^{e_2-1}w_2, \\ &\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots \\ &w_t,\ (\lambda-r_t)w_t,\ \cdots,\ (\lambda-r_t)^{e_t-1}w_t. \end{aligned}$$

于是，线性变换σ在这样得到的基底上的系数矩阵为

$$C=\begin{pmatrix} C_1 & & & \\ & C_2 & & \\ & & \ddots & \\ & & & C_t \end{pmatrix},$$

其中

$$C_i=\begin{pmatrix} r & 1 & 0 & \cdots & 0 & 0 \\ 0 & r_i & 1 & \cdots & 0 & 0 \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & 0 & \cdots & r_i & 1 \\ 0 & 0 & 0 & \cdots & 0 & r_i \end{pmatrix},\quad i=1,\ 2,\ \cdots,\ t.$$

我们称矩阵 C 为线性变换 σ 的 *Jordan* 标准形矩阵。

为了求出一个线性变换 σ 的 *Jordan* 标准形矩阵，只要求出模 V 的初等因子组即可。一般地，把不变因子 $d_1(\lambda)$，$d_2(\lambda)$，…，$d_s(\lambda)$ 表成标准分解式：

$$d_1(\lambda)=p_1^{k_{11}}(\lambda)p_2^{k_{12}}(\lambda)\cdots p_{t_1}^{k_{1t_1}}(\lambda),$$

$$d_2(\lambda)=p_1^{k_{21}}(\lambda)p_2^{k_{22}}(\lambda)\cdots p_{t_2}^{k_{2t_2}}(\lambda),$$

$$\cdots\quad\cdots\quad\cdots\quad\cdots\quad\cdots$$

$$d_s(\lambda)=p_1^{k_{s1}}(\lambda)p_2^{k_{s2}}(\lambda)\cdots p_{t_s}^{k_{st_s}}(\lambda),$$

那么元素的幂 $p_j^{k_{ij}}(\lambda)$，除去指数为 0的，就是所要求的全部初等因子。在前面的例题里，不变因子

$\lambda-1$，$(\lambda-1)^2$

已是初等因子。于是 σ 的 *Jordan* 标准形矩阵为

$$C=\begin{pmatrix}1 & 0 & 0\\ 0 & 1 & 1\\ 0 & 0 & 1\end{pmatrix}$$

以上关于线性变换 σ 的标准形矩阵的讨论表明，如果把域 F 上的 n 阶方阵按相似关系加以分类，那么每一个类里都有唯一的一个有理标准形矩阵（也叫这个类里任一矩阵的有理标准形），而且不同的类里的有理标准形也不同。换句话说就是

A 与 B 相似 $\Longleftrightarrow$ A 与 B 的有理标准形相同。

再有，如果 $F[\lambda]$ 中多项式都能分解成一次因式的乘积，那么在相似分类之下还存在另外一种标准形矩阵，即 *Jordan* 标准形。并且也有相应的一个充分必要条件，即

A 与 B 相似 $\Longleftrightarrow$ 在不计对角线上小块的次序的意义下，A 与 B 的 *Jordan* 标准形相同。显然，A 的有理标准形由特征矩阵

$\lambda I-A$的不变因子所决定；A的Jordan标准形则由$\lambda I-A$的初等因子——一次式的幂所决定.

习　　题

1. 决定阶为360的不同构的交换群.

2. 验证矩阵

$$A=\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ -2 & 0 & 0 & 1 \\ -2 & 0 & -1 & 2 \end{pmatrix}$$

的特征多项式在有理数域上是一次式的乘积，进而决定A的有理标准形和Jordan标准形. 再求出使A相似于各标准形的过渡矩阵.

3. 设F是域，A，$B\in M_n(F)$. 证明：A与B相似$\Longleftrightarrow$ $\lambda I-A$与$\lambda I-B$相抵.

4. 证明：任意矩阵A相似于它的转置矩阵A'.

5. 证明：线性变换σ所决定的$F[\lambda]$—模V是循环的当且仅当σ的特征多项式$f(\lambda)$是σ的最低多项式.

6. 证明：任何一个幂零矩阵A(即$A^k=0$)必相似于矩阵

$$\begin{pmatrix} N_1 & & & 0 \\ & N_2 & & \\ & & \ddots & \\ 0 & & & N_s \end{pmatrix},$$

其中N_i为如下形式的矩阵：

$$N_i=\begin{pmatrix} 0 & 1 & 0 & \cdots & 0 & 0 \\ 0 & 0 & 1 & \cdots & 0 & 0 \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & 0 & \cdots & 0 & 1 \\ 0 & 0 & 0 & \cdots & 0 & 0 \end{pmatrix}\quad i=1,\ 2,\ \cdots,\ s.$$

7. 设 p 为素数，$F=Z_p$。证明：F上的两个 p 阶方阵

$$\begin{pmatrix} 0 & 1 & 0 & \cdots & 0 & 0 \\ 0 & 0 & 1 & \cdots & 0 & 0 \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & 0 & \cdots & 0 & 1 \\ 1 & 0 & 0 & \cdots & 0 & 0 \end{pmatrix} \text{与} \begin{pmatrix} 1 & 1 & 0 & \cdots & 0 & 0 \\ 0 & 1 & 1 & \cdots & 0 & 0 \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & 0 & \cdots & 1 & 1 \\ 0 & 0 & 0 & \cdots & 0 & 1 \end{pmatrix}$$

相似。

8. 证明：实数域R上任意一个 n 阶方阵 A 均相似于一个分块对角形阵，使对角线上的小块为以下两种形式之一：

$$\begin{pmatrix} r & 1 & 0 & \cdots & 0 & 0 \\ 0 & r & 1 & \cdots & 0 & 0 \\ \cdot & \cdot & \cdot & \cdots & \cdot & \cdot \\ 0 & 0 & 0 & \cdots & r & 1 \\ 0 & 0 & 0 & \cdots & 0 & r \end{pmatrix}$$

或

$$\begin{pmatrix} 0 & 1 & 1 & 0 & & & & & & \\ -b & a & 0 & 1 & & & & & & \\ & & 0 & 1 & 1 & 0 & & & & \\ & & -b & a & 0 & 1 & & & & \\ & & & & & \ddots & & & & \\ & & & & & & 0 & 1 & 1 & 0 \\ & & & & & & -b & a & 0 & 1 \end{pmatrix},$$

使得$a^2<4b$，其中未标出的元素都等于 0。

9. 设 R 为交换环，e_1，e_2，$\cdots$，e_n为自由模$R^{(n)}$的任意一个基底。令 η 为$R^{(n)}$的任意一个模自同态，使$\eta e_i=\sum\limits_{j=1}^{n}a_{ij}e_j$，$i=1$，2，$\cdots$，$n$。于是象域的情形一样，使$R^{(n)}$成为一个$R[\lambda]$上的模，即规定：$\lambda x=\eta x$，$\forall x\in R^{(n)}$。证明$Cayley$ 定理成立，即$f(A)=0$。其中$A=(a_{ij})$，$f(\lambda)=|\lambda I-A|$。

§6 主理想环上有限生成模的自同态环

在第三节里我们讨论了用矩阵来刻划模的同态映射。特别地，对自由模的自同态给出了它的矩阵表示定理。容易想到这是高等代数中关于有限维线性空间的线性变换的矩阵表示理论的简单推广。现在，我们将把线性变换的矩阵表示理论进一步推广到主理想环 D上的有限生成模M的情况，在结构定理（§ 4 定理 1）的基础上研究自同态环 $End_D M$的矩阵表示问题。

设D为主理想环，M为D上的有限生成模。$End_D M$为M的全自同态环。

根据§ 4 定理 1，M有标准分解式：

$$M = Dz_1 \oplus Dz_2 \oplus \cdots \oplus Dz_s,$$

$$ann z_1 \supseteq ann z_2 \supseteq \cdots \supseteq ann z_s;$$

或者是

$$ann z_1 = (d_1),\ ann z_2 = (d_2),\ \cdots,\ ann z_s = (d_s),$$

使得

$$d_1 \setminus d_2 \setminus \cdots \setminus d_s.$$

令

$$ann z_1 \neq 0,\ \cdots,\ ann z_r \neq 0,\ ann z_{r+1} = \cdots = ann z_s = 0.$$

我们考察M的任意一个自同态 η。可令

$$\eta(z_1) = w_1,\ \eta(z_2) = w_2,\ \cdots,\ \eta(z_s) = w_s.$$

即自同态 η 作用在生成组 $z_1, z_2, \cdots, z_s$ 上的象依次为M中的 s 个元素：

$$w_1,\ w_2,\ \cdots,\ w_s.$$

于是，对于M中的任意一个元素 x，它在 η 之下的象为：

若 $x = a_1 z_1 + a_2 z_2 + \cdots + a_s z_s$,

则

$$\eta(x)=a_1w_1+a_2w_2+\cdots+a_sw_s.$$

并且还有，对于每一个w_i都有

$$d_iw_i=d_i\eta(z_i)=\eta(d_iz_i)=\eta(0)=0,$$

$\Longrightarrow annw_i\supseteq annz_i$.

反之，如果 $w_1, w_2, \cdots, w_s$是M中的s个元素具有性质：

$annw_1\supseteq annz_1,\ annw_2\supseteq annz_2,\ \cdots,\ annw_s\supseteq annz_s,$

则有

$$\sum_{i=1}^{s}a_iz_i=\sum_{i=1}^{s}b_iz_i\Longrightarrow\sum_{i=1}^{s}a_iw_i=\sum_{i=1}^{s}b_iw_i$$

由此可知，规则

$$\eta:\sum_{i=1}^{s}a_iz_i\longmapsto\sum_{i=1}^{s}a_iw_i,$$

合理地定义了M的一个变换。并且不难验证：$\eta\in End_DM$，亦即这样定义的η必为模M的自同态。

把以上讨论归纳起来，我们已经得到如下的基本事实。

命题 1 设

$$W=\{(w_1,w_2,\cdots,w_s)\mid w_i\in M,\text{使}annw_i\supseteq annz_i\}.$$

则有规则：

$$\varphi:\eta\longmapsto(w_1,w_2,\cdots,w_s)$$

是End_DM与W之间的一个双射。∎

设$\eta\in End_DM$，使

$$\varphi:\eta\longmapsto(w_1,w_2,\cdots,w_s).$$

令

$$\eta(z_1)=w_1=b_{11}z_1+b_{12}z_2+\cdots+b_{1s}z_s,$$
$$\eta(z_2)=w_2=b_{21}z_1+b_{22}z_2+\cdots+b_{2s}z_s,$$
$$\vdots$$
$$\eta(z_s)=w_s=b_{s1}z_1+b_{s2}z_2+\cdots+b_{ss}z_s.$$

对此我们采用简洁的记法如下：

$$\eta\begin{pmatrix} z_1 \\ z_2 \\ \vdots \\ z_s \end{pmatrix}=\begin{pmatrix} b_{11} & b_{12} & \cdots & b_{1s} \\ b_{21} & b_{22} & \cdots & b_{2s} \\ \cdots & \cdots & \cdots & \cdots \\ b_{s1} & b_{s2} & \cdots & b_{ss} \end{pmatrix}\begin{pmatrix} z_1 \\ z_2 \\ \vdots \\ z_s \end{pmatrix}$$

称s阶方阵$B=(b_{ij})$为自同态η关于生成组$z_1, z_2, \cdots, z_s$的表示矩阵。

现在我们指出矩阵B的如下之特性。

（1）由$annz_i=(d_i)$，可知B的第i行元素

$$b_{i1}, b_{i2}, \cdots, b_{is}$$

可用元素$b'_{i1}, b'_{i2}, \cdots, b'_{is}$来代替，此处

$$b'_{i1}\equiv b_{i1} \pmod{d_1}$$
$$b'_{i2}\equiv b_{i2} \pmod{d_2}$$
$$\vdots$$
$$b'_{is}\equiv b_{is} \pmod{d_s}$$

一般地，即有

$$b'_{ij}\equiv b_{ij} \pmod{d_j},\ j=1, 2, \cdots, s.$$

（2）由$annw_i\supseteq annz_i$，即$d_iw_i=0$，则有

$$d_ib_{i1}z_1+d_ib_{i2}z_2+\cdots+d_ib_{is}z_s=0$$
$$\Longrightarrow d_ib_{i1}z_1=0,\ d_ib_{i2}z_2=0,\ \cdots,\ d_ib_{is}z_s=0,$$
$$\Longrightarrow d_1\diagdown d_ib_{i1},\ d_2\diagdown d_ib_{i2},\ \cdots,\ d_s\diagdown d_ib_{is},$$
$$\Longrightarrow d_ib_{i1}=c_{i1}d_1,\ d_ib_{i2}=c_{i2}d_2,\cdots,d_ib_{is}=c_{is}d_s,$$

即有$c_{i1}, c_{i2}, \cdots, c_{is}\in D$，使得

$$d_ib_{ij}=c_{ij}d_j,\ 1\leqslant i,\ j\leqslant s.$$

这$s\times s$个等式可以用矩阵的形式集中的、鲜明的表达出来，即有

$$\begin{pmatrix} d_1 & & & \\ & d_2 & & \\ & & \ddots & \\ & & & d_s \end{pmatrix}\begin{pmatrix} b_{11} & b_{12} & \cdots & b_{1s} \\ b_{21} & b_{22} & \cdots & b_{2s} \\ \cdots & \cdots & \cdots & \cdots \\ b_{s1} & b_{s2} & \cdots & b_{ss} \end{pmatrix}=\begin{pmatrix} c_{11} & c_{12} & \cdots & c_{1s} \\ c_{21} & c_{22} & \cdots & c_{2s} \\ \cdots & \cdots & \cdots & \cdots \\ c_{s1} & c_{s2} & \cdots & c_{ss} \end{pmatrix}\begin{pmatrix} d_1 & & & \\ & d_2 & & \\ & & \ddots & \\ & & & d_s \end{pmatrix}$$

还可写成

$$diag\{d_1, d_2, \cdots, d_s\}B = Cdiag\{d_1, d_2, \cdots, d_s\} \quad (*)$$

其中 $C=(c_{ij})$。而且容易指出，如果矩阵 B满足条件（*），那么 $B_1 = B + Tdiag\ \{d_1, d_2, \cdots, d_s\}$ 也满足条件（*），其中 $T \in M_s(D)$ 。

令

$$R = \{B \in M_s(D) \mid B\text{满足条件}（*）\}。$$

容易验证，R是$M_s(D)$ 的一个子环，并且对任意一个 $B \in R$，用

$$\eta \begin{pmatrix} \\ z_2 \\ \vdots \\ z_s \end{pmatrix} = B \begin{pmatrix} \\ z_2 \\ \vdots \\ z_s \end{pmatrix}$$

恰好定义模M的一个自同态 η。

这样，子环 R中之矩阵恰是 End_dM 中一切自同态的全部表示矩阵。即

$$\varphi : B \longmapsto \eta$$

是从 R到 End_DM 的一个满射。并且此 φ 是环的反同态。

进而还有

$$\varphi(B) = 0 \Longleftrightarrow B = Tdiag\{d_1, d_2, \cdots, d_s\}$$

即反同态映射 φ 的核 $ker\varphi = K$是环 R中一切满足条件

$$B = Tdiag\{d_1, d_2, \cdots, d_s\} \qquad (**)$$

的矩阵 B所成之理想，$T \in M_s(D)$。

把以上的讨论归纳起来，可以得到如下的结论。即

命题 2 设

$$M = Dz_1 \oplus Dz_2 \oplus \cdots \oplus Dz_s,$$

$$annz_i = (d_i), \quad d_i \diagdown d_j, \quad i < j,$$

是 M 的标准分解式。那么 M 的自同态环 End_DM 反同态于商环 R/K，其中R是满足条件（*）的矩阵组成的全阵环 $M_s(D)$ 的子环，K是满足条件（**）的矩阵组成的R之理想。∎

特别地，如果M是D—自由模，即$(d_i)=\{0\}$，这时则有$R=M_s(D)$，$K=\{0\}$。如果$s=1$，即$M=Dz$是循环模，这时$B=(b)$，$b\in D$。由D的交换性，条件（*）将自然被满足。故而$R=D$，$K=(d)=annz$。于是

$$D/(d)\simeq End_D M。$$

下面我们进一步揭示表示矩阵B的具体特征。

由条件$d_1\backslash d_2\backslash\cdots\backslash d_r\neq 0$，$d_{r+1}=\cdots=d_s=0$，则有

（1）若$i\geqslant j$，则$d_j\backslash d_i$。于是条件

$$d_i b_{ij}\equiv 0\pmod{d_j}$$

对任意的b_{ij}都能被满足。所以，B中(i,j)位置的元素b_{ij}可以是任意的。

（2）若$i\leq r$，$j>r$。则$d_j=0$，$d_i\neq 0$。于是条件

$$d_i b_{ij}\equiv 0\pmod{d_j}$$

只有当$b_{ij}=0$时才能被满足。所以，B中(i,j)位置的元素$b_{ij}=0$。

（3）若$i>r$，$j>r$。则$d_j=0$，$d_i=0$。于是条件

$$d_i b_{ij}\equiv 0\pmod{d_j}$$

对任意的b_{ij}都能被满足。所以，B中(i,j)位置的元素b_{ij}可以是任意的。

（4）若$i<j\leq r$，则条件

$$d_i b_{ij}\equiv 0\pmod{d_j}$$

表明$d_j\backslash d_i b_{ij}$。于是存在元素c_{ij}，使

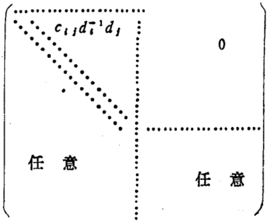
$$d_i b_{ij}=c_{ij}d_j$$

此式可以简记作：$b_{ij}=c_{ij}d_i^{-1}d_j$。

综合以上各种情况，R中矩阵$B=(b_{ij})$之元素可以具体的表明如下：

$$B=\begin{pmatrix} c_{11} & c_{12}d_1^{-1}d_2 & \cdots & c_{1r}d_1^{-1}d_r & 0 & \cdots & 0 \\ c_{21} & c_{22} & \cdots & c_{2r}d_2^{-1}d_r & 0 & \cdots & 0 \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ c_{r1} & c_{r2} & \cdots & c_{rr} & 0 & \cdots & 0 \\ c_{r+1\,1} & c_{r+1\,2} & \cdots & c_{r+1\,r} & c_{r+1\,r+1} & \cdots & c_{r+1\,s} \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ c_{s1} & c_{s2} & \cdots & c_{sr} & c_{s\,r+1} & \cdots & c_{ss} \end{pmatrix}$$

或者可以粗略地表成：

$B=$ 

，

其中标出之 c_{ij} 均为任意元素。当 $i<j\leq r$时，（i，j）位置的元素 $b_{ij}=c_{ij}d_i^{-1}d_j$。

进而，分析$B\in K$的充分必要条件是什么。或者说，指出R中之矩阵 B属于反同态 φ 的核 $ker\varphi=K$ 的特征。

由前面的讨论，已知

$B\in K\Longleftrightarrow B=Tdiag\{d_1,\ d_2,\ \cdots,\ d_s\}$

$\Longleftrightarrow B$的第 i 列元素均被 d_i所整除。

从而有

（1）若$j>r$，则 $d_j=0$。于是，K中的矩阵B其第 r 列以后各列必均为0。

（2）若 $i\geqslant j$，$j\leq r$，于是$d_j\diagdown c_{ij}$。

（3）若 $i<j\leq r$，于是 b_{ij} 应被 d_j所整除，即有

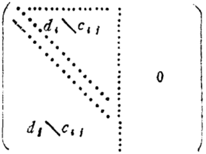
$$b_{ij}=q_{ij}d_j.$$

由此可得

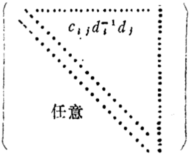
$$b_{ij}=c_{ij}d_i^{-1}d_j=q_{ij}d_j\Longrightarrow c_{ij}d_i^{-1}=q_{ij}$$

$$\Longrightarrow c_{ij}=q_{ij}d_i\Longrightarrow d_i\diagdown c_{ij}.$$

这样，K中的矩阵应具以下形式：



最后指出，当M是扭模时，则有 $s=r$。此时，表示矩阵B“收缩”成左上角那块r阶方阵。即B中被划分的四个区域简化为两个区域：对角线及其下部；对角线的上部：



其中 c_{ij}为D中之任意元素。

以上对主理想环D上的有限生成模M的自同态环End_DM之表示矩阵给出了具体的刻划，而且指出了零自同态的表示矩阵之特征。在此基础上，对由n维线性空间V的一个线性变换σ所诱导出来的$F[\lambda]$—模V给出一些重要的结果。

因为$F[\lambda]$—模V是扭模，所以一切 $d_i\neq 0$ （或$d_i(\lambda)\neq 0$）。如上所述，这时矩阵B已收缩为两个区域，于是可以做如下之处理。

（1）对 $i \geqslant j$，即对角线上及其下部的元素 c_{ij}，可用 $(mod\ d_j)$ 之合同元素 c'_{ij}来代替 c_{ij}。即可令

$$c_{ij}=q_{ij}d_j+c'_{ij},\ degc'_{ij}<degd_j=n_j.$$

（2）类似地，对 $i<j$，即对角线上部的元素 $c_{ij}d_i^{-1}d_j$，可令

$$c_{ij}=q_{ij}d_i+c'_{ij},\ degc'_{ij}<degd_i=n_i.$$

当把R中的矩阵 B 简化成满足上述之条件（1）与（2）时（实际上就是降低B中各元素的次数，使之低于相应的 d_i 的次数），则称 B为正规化的矩阵。

对表示矩阵 B 之所以按此方式加以正规化，因为：

$B\in K \Longleftrightarrow B$的对角线上及其下部的元素按列（$mod\ d_j$）合同，对角线上部的元素按行（$mod\ d_i$）合同。因此，$R$中的正规化矩阵做成的子集$S$与自同态环$End_{F(\lambda)}V$之间可以建立起一个一一对应

$$\psi: B \longmapsto \eta,\ B\in S.$$

这样，S与$End_{F(\lambda)}V$都可以自然地看成是基础域F上的线性空间，而且在双射 ψ之下二者是同构的，即

$$S\overset{\psi}{\simeq}End_{F(\lambda)}V.$$

诚然，这里是做为域 F上线性空间的同构。从而可得

$$dim_F S=dim_F EndV.$$

命题 3 设V是域F上的n维线性空间，σ 是 V 的给定的一个线性变换，τ为V的任意一个线性变换。则有

τ是$F[\lambda]$—模V的一个自同态$\Longleftrightarrow \sigma\tau=\tau\sigma$，其中 $F[\lambda]$—模 V 是由 σ 诱导而成的。

做为一个习题，把命题 3 的证明留给读者去做。▮

通过命题 3 便可计算出与域 F 上一个给定的方阵 A（看成 $\sigma \longmapsto A$）可交换的一切矩阵（组成 F上的一个线性空间）之维数 t。因为 $t=dimS$，

具体计算如下：

设 $S_{ij}(1\leq i,\ j\leq s)$表示除（$i$，$j$）位置之外，其它元素均为 0，而（$i$，$j$）位置元素是任意的正规化矩阵。于是，对每一对$i$与$j$，一切$S_{ij}$做成$S$的一个子空间，并且有线性空间的直和

$$S=\bigoplus S_{ij}.$$

从而可得

（1）当 $i\geqslant j$时，$dim\{S_{ij}\}=n_j$，

（2）当 $i<j$ 时，$dim\{S_{ij}\}=n_i$。

故而

$$\begin{aligned}dimS&=s\cdot n_1+(s-1)n_2+\cdots+2n_{s-1}+1\cdot n_s+\\&\quad+(s-1)n_1+(s-2)n_2+\cdots+2n_{s-2}+1\cdot n_{s-1}\\&=\sum_{j=1}^{s}(s-j+1)n_j+\sum_{i=1}^{s-1}(s-i)n_i\\&=\sum_{j=1}^{s}(2s-2j+1)n_j.\end{aligned}$$

用矩阵语言来表述以上这个等式的结果，则有

定理 1 （*Frobenius*）设$A\in M_n(F)$，$d_1(\lambda)$，$d_2(\lambda)$，…，$d_s(\lambda)$ 是 $\lambda I-A$ 的不等于 1 的不变因子。令

$$degd_i(\lambda)=n_i,\quad i=1,\ 2,\ \cdots,\ s.$$

那么与A可交换的一切 n 阶方阵组成F上的一个线性空间S，其维数

$$dimS=\sum_{j=1}^{s}(2s-2j+1)n_j.\ \blacksquare$$

推论 如果$F[\lambda]$—模 V 是循环的： $V=F[\lambda]z$，就说线性变换σ是循环的。那么，σ是循环的当且仅当与σ可交换的一切线性变换恰为σ的全部多项式。即

$$\sigma\tau=\sigma\tau\Longleftrightarrow\tau=f(\sigma),\ f(\lambda)\in F[\lambda],$$

或者，令S_σ表示与 σ 可交换的一切线性变换τ组成的线性空间，

则有 $S_\sigma = F[\sigma]$。

事实上，σ 是循环的 $\Longleftrightarrow s=1$，即 $V=F(\lambda)z_1$。于是 $d_s(\lambda)$（即 $d_1(\lambda)$）是 σ 的最低多项式 $m(\lambda)$。因而，σ 的多项式集合 $F[\sigma]$，做为 F 上的线性空间，其维数恰好等于 $n_1 = deg d_1(\lambda)$。显然，$F[\sigma] \subseteq S_\sigma$，即 σ 的多项式必与 σ 可交换。这样，为了此式之等号成立，当且仅当 $s=1$ 即足。

由维数公式，当 $s=1$ 时，$dim S = n_1$，从而可得 $F[\sigma]=S_\sigma$。如果 $s>1$，则有

$$dim S = \sum_1^s (2s-2j+1)n_j > \sum_1^s n_j > n_1,$$

$$\Longrightarrow F[\sigma] \subsetneqq S_\sigma，\text{或是} F[\sigma] < S_\sigma.$$

总之，推论被证明了。▌

最后，给出关于自同态环 $End_D M$ 的中心的一个结果，来结束我们的讨论。

定理 2 $End_D M$ 的中心恰是一切"相似自同态" σ 所组成的子环 C：

$$\sigma: x \mapsto ax \; \forall x \in M,$$

a 为 D 中取定的任意一个元素。

证 显然，每一个"相似自同态" σ 均属于自同态环 $End_D M$ 的中心。反之，设 γ 为 $End_D M$ 的中心里的一个元素。

我们考虑一组特殊的自同态：

$$e_{ts}(z_i) = \begin{cases} z_t, & \text{当 } t=s \text{ 时}, \\ 0, & \text{当 } t \neq s \text{ 时}, \; i=1, 2, \cdots, s \end{cases}$$

具体地写出来就是

$$\varepsilon_{1s}: \begin{array}{ccccc} z_1, & z_2, & \cdots, & z_{s-1}, & z_s, \\ \downarrow & \downarrow & & \downarrow & \downarrow \\ 0, & 0, & \cdots, & 0, & z_1, \end{array}$$

$$\varepsilon_{2s}:\begin{array}{ccccc} z_1, & z_2, & \cdots, & z_{s-1}, & z_s, \\ \downarrow & \downarrow & & \downarrow & \downarrow \\ 0, & 0, & \cdots, & 0, & z_2, \end{array}$$

$$\cdots\cdots\cdots\cdots\cdots\cdots$$

$$\varepsilon_{ss}:\begin{array}{ccccc} z_1, & z_2, & \cdots, & z_{s-1}, & z_s, \\ \downarrow & \downarrow & & \downarrow & \downarrow \\ 0, & 0, & \cdots, & 0, & z_s, \end{array}$$

于是

$$\gamma z_s=\gamma(\varepsilon_{ss}z_s)=\varepsilon_{ss}(\gamma z_s)=\varepsilon_{ss}(a_1z_1+a_2z_2+\cdots+a_sz_s)$$
$$=a_s\varepsilon_{ss}z_s=a_sz_s$$

同样可得

$$\gamma z_i=a_sz_i,\ i=1,\ 2,\ \cdots,\ s-1.$$

由此可见，对M中的任意一个元素x，都有

$$\gamma x=a_sx.$$

这就是说中心里的元素γ恰好是一个“相似自同态”。故而C就是End_DM的中心。∎

例 取$F=Q$为有理数域，σ为Q上三维空间$V=[u_1,\ u_2,\ u_3]$的一个线性变换。令

$$\sigma\begin{pmatrix}u_1\\u_2\\u_3\end{pmatrix}=A\begin{pmatrix}u_1\\u_2\\u_3\end{pmatrix}$$

其中

$$A=\begin{pmatrix}1&0&0\\0&0&1\\0&-1&2\end{pmatrix}$$

求与A可交换的一切三阶方阵。

解 (一) 把V做为$Q[\lambda]$—模来看，则由特征矩阵为

$$\lambda I-A=\begin{pmatrix}\lambda-1&0&0\\0&0&-1\\0&1&\lambda-2\end{pmatrix},$$

可知不变因子为 1，$\lambda-1$，$(\lambda-1)^2=\lambda^2-2\lambda+1$，于是，由分解定理，有标准分解式

$$V=Q[\lambda]f_1\oplus Q[\lambda]f_2,$$

$$\mathrm{ann} f_1=((\lambda-1)),\ \mathrm{ann} f_2=((\lambda-1)^2).$$

即有 $d_1(\lambda)=\lambda-1$，$d_2(\lambda)=\lambda^2-2\lambda+1$，$n_1=1$，$n_2=2$.

这样，R中之正规化矩阵有以下形式：

$$\begin{pmatrix} b_{11} & b_{12}(\lambda-1) \\ b_{21} & b_{22}+b'_{22}\lambda \end{pmatrix},\ b_{ij},\ b'_{22}\in Q.$$

与此正规化矩阵对应的线性变换 τ 为

$$\begin{cases} \tau f_1=b_{11}f_1+b_{12}(\lambda-1)f_2, \\ \tau f_2=b_{21}f_1+(b_{22}+b'_{22}\lambda)f_2. \end{cases}$$

由标准分解式中的生成元 f_1，f_2 还原得出V在Q上的基底为

$$f_1,\ f_2,\ \lambda f_2.$$

此中 f_2，λf_2，就是 $Q[\lambda]f_2$ 看成 Q 上的线性空间时的一组基底。

由此进而便可算出做为Q上线性空间 V 的线性变换 τ 在基底 f_1，f_2，λf_2上的系数矩阵B：

$$\tau\begin{pmatrix} f_1 \\ f_2 \\ \lambda f_2 \end{pmatrix}=B\begin{pmatrix} f_1 \\ f_2 \\ \lambda f_2 \end{pmatrix},$$

此处

$$\tau f_1=b_{11}f_1-b_{12}f_2+b_{12}\lambda f_2,$$
$$\tau f_2=b_{21}f_1+b_{22}f_2+b'_{22}\lambda f_2,$$
$$\tau\lambda f_2=b_{21}f_1-b'_{22}f_2+(b_{22}+2b'_{22})\lambda f_2$$

即有

$$B=\begin{pmatrix} b_{11} & -b_{12} & b_{12} \\ b_{21} & b_{22} & b'_{22} \\ b_{21} & -b'_{22} & b_{22}+2b'_{22} \end{pmatrix}$$

由于σ关于基底 f_1，f_2，λf_2 的系数矩阵就是A，所以与 A 可交换的矩阵其一般形式就是上述的矩阵 B。

习　　题

1. 证明命题3.

2. 设 G为有限交换群，它是阶数依次为n_1，n_2，…，n_s的循环群的直和，其中 $n_i \setminus n_j (i<j)$. 证明：G 的自同态之个数等于

$$N = \prod_{j=1}^{s} n_j^{(2s-2j+1)}$$

3. 在$M_5(Q)$ 里求出与矩阵

$$\begin{pmatrix} 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \end{pmatrix}$$

可交换的一切矩阵。

4. 在$M_4(Q)$ 里求出与矩阵

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 1 & -3 & 3 \end{pmatrix}$$

可交换的一切矩阵。

5. 证明：域上有限维线性空间的一个线性变换 σ 是循环的当且仅当与 σ 可交换的线性变换环是交换环。